KAAP AGULHAS MUNISIPALITEIT
CAPE AGULHAS MUNICIPALITY
U MASIPALA WASECAPE AGULHAS

# INLIGTINGSTEGNOLOGIE (IT)-BELEID

MET INBEGRIP VAN DIE VOLGENDE :

## DATA- EN STELSELSEKERHEIDBELEID

## NETWERKSEKERHEIDBELEID

## INTERNET-, INTRANET-, EKSTRANET- EN E-POSBELEID

---

INHOUD

# DATA- EN STELSELSEKERHEIDBELEID

# NETWERKSEKERHEIDBELEID

# INTERNET-, INTRANET-, EKSTRANET- EN E-POSBELEID

# DATA-EN STELSELSEKERHEIDBELEID

## VOORWOORD

Inligting en inligtingstelsels is van kritiese en noodsaaklike belang vir die Munisipaliteit. Die gebrek aan betroubare inligting kan die Munisipaliteit se finansiële posisie en reputasie nadelig raak. Gevolglik stel hierdie Beleid die minimum vereistes en die verantwoordelikheid waaraan alle werknemers, tydelike werknemers, kontrakteurs en bestuur moet voldoen om die Munisipaliteit se inligting te beveilig.

Hierdie Beleid sit die benadering uiteen wat gevolg moet word om te verseker dat inligtingsbates behoorlik beskerm word teen verskeie bedreigings soos foute, bedrog, verduistering, sabotasie, terrorisme, afpersing, skending van privaatheid, diensonderbreking, diefstal en natuurlike rampe, hetsy intern of ekstern, doelbewus of toevallig.

Dit is die plig van ***KAAP AGULHAS*** Munisipaliteit se Bestuur om alle inligting en inligtingstelsels te bewaar, verbeter en verantwoordelikheid daarvoor te aanvaar. Daarbenewens moet hulle toesien dat inligtingsbates beveilig word op ’n wyse wat minstens so veilig is as die van ander organisasies in dieselfde bedryf wat dieselfde soort inligting hanteer. Ten einde hierdie doelwit te bereik, moet jaarlikse oorsigte van die risiko’s vir die Munisipaliteit se inligtingsbates uitgevoer word. So ook moet Bestuur spoedig korrektiewe optrede neem om die munisipaliteit se blootstelling te verminder indien ’n sekerheidsinsident of ouditbevinding daarop dui dat die sekerheid van inligting of inligtingstelsels onvoldoende is.

Die Munisipaliteit se inligting moet beskerm word op ’n wyse wat geskik is vir die sensitiwiteit, waarde en kritieke aard van die inligting. Sekerheidsmaatreëls moet dus gevolg word ongeag die media waarop inligting gestoor word, die stelsel wat dit verwerk of die metodes waardeur dit vervoer word. Hierdie beskerming sluit beperking van toegang tot inligting in, op grond van die beginsel van noodsaaklike kennis.

Besluitneming in die Munisipaliteit is ook krities afhanklik van inligting, aangesien Bestuur moet kan staatmaak op die integriteit van inligting ten opsigte van akkuraatheid, tydigheid, relevansie, volledigheid, kritiekheid, ens. Dit is ’n belangrike bestuursaktiwiteit om bewus te wees van sodanige inligting en om dit fyn te kan instel.

---

Inligtingsekerheid vereis die deelname en steun van alle personeel (insluitende konsultante, kontrakteurs en tydelike werknemers) wat voldoende opleiding- en ondersteuningsprosedures / beleid moet ontvang om hulle in staat te stel om die Munisipaliteit se inligtingsbates behoorlik te beskerm en te bestuur.

Dit is die verantwoordelikheid van alle Munisipale personeel om enige programmatuurwanfunksie, sekerheidsinsidente, vermeende virusse, foute, swakhede of bedreigings wat waargeneem of vermoed word aan stelsels of dienste, so spoedig moontlik by die Hulplessenaar, Netwerkadministrateur of Bestuurder wat vir inligting/stelselsekerheid verantwoordelik is, aan te meld om die omvang en koste van insidente en wanfunksies te kwantifiseer en te moniteer.

## DOEL VAN DIE BELEID

Hierdie dokument omskryf die Beleid van die Munisipaliteit vir die toepassing van inligtingsekerheid om die Munisipaliteit se korporatiewe inligting, inligtingstelsels en toepassings te beskerm teen alle bedreigings wat die vertroulikheid, integriteit en beskikbaarheid daarvan kan bedreig.

Die doelwit van inligtingsekerheid is om sakekontinuïteit te verseker en skade aan die organisasie te minimaliseer deur die impak van sekerheidsinsidente te voorkom en tot die minimum te beperk. Die doel van hierdie Beleid is om die Munisipaliteit se inligtingsbates ten opsigte van Vertroulikheid, Integriteit en Beskikbaarheid te beskerm.

## BESTEK

Hierdie Beleid is van toepassing op alle kantore en gebruikers van inligting in die Munisipaliteit. Dit geld vir alle apparatuurplatforms, alle departemente, sake-eenhede en alle vennote, personeel en kontrakteurs van die Munisipaliteit.

## ALGEMENE RIGLYNE

Dit is die verantwoordelikheid van alle Bestuurders in die Munisipaliteit om toe te sien dat personeel in hul Departemente die IT-beleid van die Munisipaliteit ontvang en verstaan. Daar word van personeel verwag om ’n Aanvaarding van Beleidsvoorwaardes te onderteken.

Kliënte en belanghebbendes wat toegang tot die Munisipaliteit se IT-geriewe verkry, moet ’n Aanvaarding van Beleidsvoorwaardes onderteken.

Die bestuur van die Munisipaliteit se IT-geriewe berus by die IT-afdeling en kan derdepartykontrakteurs betrek, soos diensverskaffers van die Munisipaliteit. Waar dit die geval is, moet die diensverskaffer ’n Aanvaarding van Beleidsvoorwaardes onderteken.

Toegang van nie-munisipale werknemers tot die Munisipaliteit se IT-geriewe is onderhewig aan die IT-beleid. Konsultante wat op ’n permanente grondslag in diens van die Munisipaliteit is, word vir die doeleindes van hierdie beleid as munisipale werknemers geklassifiseer.

Daar sal van deeltydse kontrakteurs en konsultante wat toegang tot munisipale IT-geriewe, infrastruktuur, stelsel en inligting mag hê, verwag word om ’n Aanvaarding van Beleidsvoorwaardes te onderteken.

## INLIGTINGSEKERHEIDSDEFINISIES

Inligtingsekerheid omvat die bestuursproses, tegnologie en versekeringsmeganismes wat departemente in staat sal stel om hul transaksies te vertrou, toe te sien dat die inligting bruikbaar is en onklaarraking as gevolg van foute, doelbewuste aanvalle of rampe behoorlik te kan weerstaan en daarvan te herstel; en dat vertroulike inligting weerhou word van diegene wat nie toegang daartoe behoort te kry nie.

# HOËVLAK-INLIGTINGSEKERHEIDSBEGINSELS

## BESKERMING

Die Munisipaliteit se inligting moet beskerm word op ’n wyse ooreenkomstig die sensitiwiteit, waarde en kritiekheid van die inligting. Sekerheidsmaatreëls moet toegepas word ongeag die media waarop inligting gestoor word (papier, transparant, rekenaarbisse, ens.), die stelsels wat dit verwerk (mikrorekenaars, spermure, stemposstelsels, ens.), of die metodes waardeur dit versprei word (elektroniese pos, mens-tot-mens gesprek, ens.). Sodanige beskerming sluit die beperking van toegang tot inligting op ’n noodsaaklik kennisbeginsel in. Munisipale Bestuur moet voldoende tyd en hulpbronne toewys om te verseker dat inligting behoorlik beskerm word.

## RISIKOBESTUUR

Bestuurders is uiteindelik verantwoordelik om te verseker dat die inligting beskerm word op ’n wyse wat aanvaarbaar is vir hoër bestuur. Ten einde hierdie doelwit te bereik, moet risiko’s geïdentifiseer word deur gereelde risiko-ontleding en die neem van korrektiewe maatreëls waar van toepassing.

## INLIGTINGSBESTUUR

Besluitneming in die Munisipaliteit is ook krities afhanklik van inligting in inligtingstelsels. Daar word van Bestuur verwag om bewus te wees van die aard van inligting wat hulle vir besluitneming gebruik (akkuraatheid, tydigheid, relevansie, volledigheid, vertroulikheid, kritiekheid, ens.).

Dit is ’n belangrike bestuursaktiwiteit om bewus te wees van sodanige inligtingseienskappe en dit fyn te kan instel.

## SAMEWERKING

Inligtingsekerheid vereis die deelname en ondersteuning van alle inligtingsgebruikers. Alle gebruikers (werknemers, konsultante, kontrakteurs, derde partye en tydelike werknemers) moet voldoende opleiding en steunmateriaal ontvang om hulle in staat te stel om Munisipale inligtingsbates te beskerm en andersins te bestuur. Opleidingsmateriaal moet oordra dat inligtingsekerheid ’n belangrike deel van die Munisipaliteit uitmaak. Opleiding en dokumentasie rakende inligtingsekerheid is die verantwoordelikheid van die Netwerkadministrateur in samewerking met ’n diensverskaffer (waar van toepassing).

## ORGANISASIE

Leiding, rigtinggewing en magtiging vir inligtingsekerheidsaktiwiteite word vir die hele organisasie in die kantoor van die Netwerkadministrateur gesentraliseer. Die kantoor is verantwoordelik vir die daarstel en handhawing van organisasie-wye sekerheidsbeleide, -standaarde, -riglyne en -prosedures. Voldoeningskontrolering om te verseker dat organisasie-eenhede funksioneer op 'n wyse wat aan hierdie vereistes voldoen, is die verantwoordelikheid van die Interne/Eksterne Ouditafdeling. Die ondersoek van stelselindringing en ander inligtingsekerheidsinsidente is die verantwoordelikheid van die Bestuurder wat vir inligting- en stelselsekerheid verantwoordelik is.

## PRIVAATHEID

Alle boodskappe wat via Munisipale rekenaar- en kommunikasiestelsels versend word, is die eiendom van die Munisipaliteit. Ten einde hierdie eiendom behoorlik in stand te hou en te bestuur, behou Bestuur die reg voor om alle data wat deur hierdie stelsel gestoor of versend word, te ondersoek. Aangesien die Munisipaliteit se rekenaar- en kommunikasiestelsels vir amptelike doeleindes voorsien word, moet werknemers geen privaatheid verwag ten opsigte van die inligting wat hulle op hierdie stelsels stoor en versend nie. Ter nakoming van die privaatvereistes wat in die Grondwet van Suid-Afrika bepaal word, sal persoonlike inligting nie aan 'n derde party openbaar gemaak word nie, tensy openbaarmaking uitdruklik deur regsprosesse vereis word.

## DERDE PARTYE

Voorwaardelik tot die bekom van toegang tot die Munisipaliteit se rekenaarnetwerk, moet elke derde party sy eie gekoppelde stelsel op 'n wyse wat met die Munisipaliteite se vereistes ooreenstem, beveilig. Die Munisipaliteit behou die reg voor om die sekerheidsmaatreëls wat op hierdie gekoppelde stelsels in werking is sonder waarskuwing te oudit. Die Munisipaliteit behou ook die reg voor om netwerkverbindings met alle derde partye wat nie aan sodanige vereistes voldoen nie, onmiddellik te beëindig.

# ALGEMEEN TOEPASLIKE BELEIDE

Die volgende Beleidsverklarings omvat die kern van die Munisipaliteit se Inligtingsekerheidsbeleid vir inligting en sal soos nodig van tyd tot tyd deur inligtingsekerheidsvoorskrifte en -standaarde ondersteun word.

## KLASSIFISERING

Inligting moet volgens vlak van sensitiwiteit gekategoriseer word en ooreenkomstig gepaste vereistes beskerm word as deel van die risikobestuursproses. Die sensitiwiteitklassifikasiestandaard moet regoor die Munisipaliteit gebruik word om te verseker dat die vlak van beskerming ooreenstem met die kontroles wat nodig is (sekerheidsmeganismes) om die inligting teen openbaarmaking te beskerm (vertroulikheid), modifisering (integriteit) en / of vernietiging (beskikbaarheid en gebruik).

## VERTROULIKHEID

Die vertroulikheid van alle data, afhangende van die inligtingsekerheidsvoorskrifte sal voor versending oor netwerke beskerm word en waar aangedui, terwyl sodanige data gestoor word.

Tensy dit deur Bestuur gemagtig word, mag inligting nie aan ongemagtigde indiwidue, entiteite of prosesse beskikbaar gestel of openbaar gemaak word nie.

Maatreëls moet geïmplementeer word om inligtingsbates teen ongemagtigde toegang, openbaarmaking, kopiëring, snuffelary, afluistering en /of diefstal te beskerm.

## BESKIKBAARHEID

Die voortgesette beskikbaarheid en bruikbaarheid van dienste ooreenkomstig die organisasie se vereistes moet verseker word deur gepaste maatreëls te implementeer om die verlies van data as gevolg van die optrede van persone, stelselonklaarraking of rampe te voorkom of daarvan te herstel.

Alle inligtingsbates moet beskerm word teen:

- Vernietiging, skade of infektering
- Weiering van gemagtigde / regmatige toegang
- Vertraging van gebruik of toegang
- Natuurrampe
- Rekenaarvirusinfeksies

## INTEGRITEIT

Die integriteit van alle data, afhangende van die klassifikasie en inligtingsekerheidsvoorskrifte moet te alle tye beskerm word voor versending oor netwerke en, waar aangedui, ook terwyl sodanige inligting gestoor word.

Alle inligtingsbates moet beskerm word teen bedreigings vir data-integriteit insluitend ongemagtigde modifisering, vernietiging en wanvoorstelling van data en / of rekenaarvirusinfeksies.

## NIE-REPUDIËRING

Alle toegang tot die Munisipaliteit se tegnologiehulpbronne is onderhewig aan positiewe identifisering en bekragtiging van die gebruiker voor toegang toegestaan word.

Maatreëls moet geïmplementeer word om die nie-repudiëring van alle finansiële transaksies ooreenkomstig amptelike wetgewing en regulasies te verseker. Prosesse moet geïmplementeer word om die nie-repudiëring van die oorsprong van sensitiewe e-pos te verseker.

## AANSPREEKLIKHEID

Maatreëls moet geïmplementeer word om te verseker dat dit moontlik is om te bepaal wie optrede geneem het, wanneer die optrede geneem is en van waar die optrede geneem is. Die maatreëls moet voldoen aan die sekerheidsvereistes wat deur die Departementele Bestuurder bepaal word.

## TOEGANGSBEHEER

Alle data en inligting moet teen ongemagtigde toegang beskerm en beveilig word. Toegang tot tegnologiehulpbronne sal slegs in lyn met die gebruiker se spesifieke verantwoordelikhede (noodsaaklike toegangbeginsel) toegeken word.

## BEKRAGTIGING

Maatreëls moet geïmplementeer word om IT-gebruikers, randapparatuur en/of programme uniek te identifiseer en om indiwiduele aanspreeklikheid te verseker. Die bekragtigingsmeganismes moet met die klassifisering van die inligting wat beskerming vereis, ooreenstem en kan byvoorbeeld die vorm van wagwoorde, identiteitskodes of biometriese identifiseringstoestelle wees.

Alle gebruikers moet toegang tot die Munisipaliteit se inligtingstelsels bekom deur minstens die gebruik van ’n unieke gebruikidentifiseringskode en geheime wagwoord. As ’n eerste verdedigingsmeganisme, moet gebruikers wagwoorde kies wat nie maklik geraai kan word nie en persoonlike wagwoorde moet nie met enige ander gebruiker gedeel word nie.

## AANMELDING VAN SEKERHEIDSINSIDENTE

Alle bekende kwesbaarhede – bykomend tot alle vermeende of bekende oortredings – moet spoedig en vertroulik aangemeld word by die Kantoor van die Netwerkadministrateur of Bestuurder wat vir inligtingsekerheid verantwoordelik is. Ongemagtigde openbaarmaking van die Munisipaliteit se inligting moet ook by die betrokke inligtingseienaars aangemeld word. Die aanmelding van sekerheidsbreuke, probleme of kwesbaarhede by enige party buite die Munisipaliteit sonder die vooraf verkreë skriftelike goedkeuring van die Kantoor van die Netwerkadministrateur is streng verbode.

Enige poging om ’n werknemer te verhoed, verhinder of af te raai of in te meng met ’n werknemer in hul pogings om ’n vermeende inligtingsekerheidsprobleem of –oortreding aan te meld, is streng verbode en gronde vir dissiplinêre optrede.

## UITSONDERINGS

Uitsluitings op grond van geldige organisasiebehoeftes kan gemotiveer word en formeel gemagtig word, in welke geval rekord van die uitsluitings gehou moet word om doeltreffende bestuurs- / beheerprosesse te fasiliteer.

## ALGEMENE VEREISTES

**Eienaarskap** – Die Departement verantwoordelik vir IT is die eienaar van die beleid.

Aansoeke om afstandbeheerde toegangsdienste sal slegs goedgekeur word vir personeel en kliënte of kontrakteurs op grond van ’n geldige werksbehoefte. Alle aansoeke moet deur die aansoeker se Bestuurder goedgekeur word en aan die Bestuurder wat vir IT-sekerheid verantwoordelik is, oorhandig word. Die Bestuurder moet alle aansoeke vir goedkeuring oorweeg na oorweging van die risiko. Toegang sal periodiek hersien word met die hulp van Menslike Hulpbronne om te verseker dat bekleërs steeds in die Munisipaliteit se diens is. Alle toegang moet minstens jaarliks deur die aansoeker se bestuurder hersien word en waar van toepassing, beëindig of opgeskort word.

As deel van die aansoekproses en voor toegang goedgekeur word, moet die aansoeker ’n Aanvaarding van IT-beleidsvoorwaardes onderteken.

’n Sentrale register moet deur die IT-afdeling bygehou word van alle gebruikers met inbel- / afstandstoegang, waarop die toegangsmagtigings aangedui word om ouditbare prosesse te fasiliteer.

Om die risiko van sekerheidsbreuke tot die minimum te beperk, moet alle gebruikers van afstandstoegangsdienste opleiding ontvang voor toegang toegelaat word. Die opleiding moet insluit wat tydens sessies toegelaat word en wat nie toegelaat word nie.

Ten einde voldoening ten opsigte van programmatuur, apparatuur en sekerheidsvereistes te verseker, moet die rekenaar wat vir die afstandstoegang gebruik word deur die Munisipaliteit verskaf word. Die gebruik van privaat (tuis-) rekenaars kan slegs toegelaat word op grond van geldige werksbehoeftes en moet as ’n afwyking van hierdie Beleid verwerk word. Die Bestuurder/Departement wat verantwoordelik is vir IT-sekerheid moet ’n sentrale register van alle afwykings byhou.

Die kliënte se afstandstoegang (rekenaar gebruik om toegang tot die Munisipaliteit se netwerk te verkry) moet anti-virusprogrammatuur en die korrekte vlak sekerheidskorreksies (“patches”) hê soos van tyd tot tyd deur die IT-funksie voorgeskryf word. ’n Proses moet deur die IT-funksie geformuleer word om die gereelde bywerking van die programmatuur /korreksies te verseker.

Toegangsvoorregte mag onder geen omstandighede na ’n ander gebruiker oorgedra word sonder om die amptelike normale aansoekprosedures te volg nie.

Die toegangsvoorregte van enige gebruikers mag nie die toegang wat verkry sou word indien die gebruiker op kantoor sou werk, oorskry nie (minste toegang / magtigingsbeginsel). Indien die versoek byvoorbeeld was om toegang tot die ‘posbus (‘mailbox’)/ kalender” te verkry, mag geen ander toegang toegestaan word nie.

Om wangebruik van ’n oop sessie deur ongemagtigde persone te verhoed, moet alle sessies outomaties na 30 minute van onaktiwiteit afgeteken word.

Die gebruikers is verantwoordelik vir beide logiese en fisiese sekerheidsmeganismes van die rekenaar wat gebruik word om die afstandstoegang te verkry. As gevolg van die risiko van diefstal, word gebruikers aangeraai om data vir beskerming onder 'n kode te stoor. Die Munisipaliteit se sekerheidsvereistes moet tydens die opleidingsessie aan gebruikers oorgedra word.

**Kommentaar**: Logiese toegangsbeheer verwys na die maatreëls wat geneem word om te verhoed dat 'n ongemagtigde persoon toegang tot jou rekenaar verkry, terwyl fisiese meganismes verwys na die fisiese maatreëls wat geneem word (eerste en tweede linie van verdediging).

Vertroulike inligting wat op afstandsrekenaars gestoor word, moet teen ongemagtigde toegang beskerm word.

Formele ooreenkomste met kliënte, vennote, kontrakteurs of derde partye is 'n vereiste en moet die beginsel insluit dat vereiste minimum standaardvoldoening verifieerbaar /ouditbaar moet wees indien afstandstoegang voorsien word.

## BEKRAGTIGINGSVEREISTES

Bekragtigingsbedieners moet gekonfigureer word om die Munisipaliteit se wagwoordstandaarde na te kom. Streng fisiese en logiese toegangsbeheer tot die bekragtigingsbedieners en kommunikasietoerusting moet toegepas word.

As 'n vereiste, moet 'n unieke gebruikers-ID en 'n wagwoord wat moeilik is om te raai, gebruik word.

Gebruikers met uitgebreide toegangsvoorregte (bv. om instandhoudingstake via 'n afstandsrekenaar te doen en toegang tot sensitiewe inligting en / of kritiese hulpbronne), mag slags toegang verkry via die Munisipaliteit se aanvaarde bekragtigingsmeganismes. (Sensitiewe inligting word omskryf as inligting wat, indien dit openbaar gemaak sou word, die Munisipaliteit, sy werksvennote en /of kliënte ernstig sal benadeel en die status van die Munisipaliteit se operasionele sekerheid in ernstige gedrang sal bring).

'n Verpligte wagwoordverandering moet tydens die eerste aantekensessie gedoen word (om die aanvanklike wagwoord te verander) en daarna elke dertig (30) dae. Die IT-funksie moet 'n proses implementeer om die veilige kommunikasie van die aanvanklike wagwoord te verseker.

Geen dubbelsessies met dieselfde bekragtigingsinligting mag toegelaat word nie.

Om die oorsprong van die verbinding te bevestig, moet terugskakelfunksies geïmplementeer word indien gebruikersidentiteit-gebaseerde bekragtiging nie gebruik word nie.

Bekragtigingsinligting tussen die gebruikers en die bekragtigingsbedieners moet deur enkripsie beskerm word.

Gebruikers wat nie meer die toegang nodig het nie (a.g.v. verandering van posbeskrywing of oorplasing) moet onmiddellik van die stelsel verwyder word. Lynbestuur moet die toegangsvoorregte van gebruikers wat bedank so spoedig moontlik na formele kennisgewing van die bedanking oorweeg. Spesiale aandag moet aan ouditaantekenlyste gegee word om te verseker dat die rekeninge nie meer aktief is nie.

Alle veranderinge aan bestaande en nuwe gebruikersrekenings / profiele moet 'n formele veranderingsbestuursproses volg.

Ten onderstuening van die inligtingsekerheidstrategie om te beskerm, op te spoor en te reageer, moet alle beskikbare ouditlyste en waarskuwingsfunksies geaktiveer word met monitering- en hersieningsproses in plek. Die verslae moet deur die IT-steun/sekerheidsfunksie hersien word en, waar van toepassing, deur die bestuurder wat vir IT-sekerheid verantwoordelik is, ondersoek / na 'n hoër vlak deurgegee word.

Die Munisipaliteit behou die reg voor om enige rekening(e) wat strydig met hierdie Beleid optree of enige ander prosedurele vereistes soos wat van tyd tot tyd geformuleer mag word, op te skort / te kanselleer.

## LEË SKERM EN LEË LESSENAARBELEID

Aan die einde van elke dag, of wanneer lessenaars / kantore onbeset is, moet enige 'Bestuursvertroulike' of 'Geklassifiseerde' inligting in lessenaars, liasseerkabinette in kantore wat aan alle personeel soos van toepassing voorsien is, toegesluit word.

Alle afvalpapier met enige sensitiewe of belangrike Munisipale inligting of data daarop, moet versnipper word of in die veilige snipperbokse wat in sekere areas geleë is, geplaas word. Hierdie soort papier moet onder geen omstandighede saam met gewone vullis in die drommetjies onder elke lessenaar weggegooi word nie.

Wanneer gebruikers hul lessenaar verlaat terwyl die rekenaar aangeskakel is, is dit noodsaaklik dat die gebruiker ALTYD hul skerm 'sluit' deur 'Ctrl Alt Delete' te druk (vir XP-bedryfstelsels) en dan 'Enter' om te bevestig dat hulle hul werkstasie wil 'sluit' of die 'Windows' knoppie + "L" druk vir "Windows Vista en Windows 7" gebruikers. Onthou dat die gebruiker 'n wagwoord nodig het om weer aan te teken.

Die sluit van die skerm verhoed nie net dat iemand anders die rekenaar wat op die gebruiker se naam aangeteken is, te gebruik nie, maar dit verhoed ook dat iemand sensitiewe inligting op die skerm kan lees.

## WAGWOORDE

Wagwoorde moet **NOOIT** aan enige-iemand bekend gemaak word nie. Indien die gebruiker vermoed dat die vertroulikheid van die wagwoord in gedrang is, moet die gebruiker dit onmiddellik verander en die Netwerkadministrateur daarvan in kennis stel.

Wagwoorde moet elke dertig (30) dae verander word; die bekragtigingsbediener moet gestel word om alle wagwoorde outomaties na dertig (3) dae te laat verstryk.

Wagwoorde moet bestaan uit karakters wat die volgende insluit:

Alfa- (alfabetletters), numeriese (heelgetalle), hoof- en kleinletters en simbole.

'n Wagwoord moet uit minstens sewe (7) karakters bestaan.

Moet nooit enige woordeboekwoorde, akronieme, verjaardagdatums, opeenvolgende syfers, familiename, voetbalspanne, datums ens. gebruik nie omdat programmatuur dit maklik kan ontsyfer (dit moet nie maklik wees om te raai nie).

Wagwoorde moet nie neergeskryf word nie, tensy dit op een of ander manier beskerm word (bv. deur 'n soort kode te gebruik en dit weg te sluit).

Die bekragtigingsbediener /stelsel sal 'n lys van tot twaalf (12) vorige wagwoorde per gebruiker in stand hou en elke nuwe wagwoord moet minstens 3 veranderinge bevat. Die doel van hierdie reël is om te verhoed dat gebruikers dieselfde wagwoord oor en oor gebruik.

## TOEGANGSBEHEERBELEID

Toegang tot stelsels sal slegs toegestaan word op grond van duidelik gevestigde werksbehoeftes, wat ooreenstem met die rolle en verantwoordelikhede van diegene aan wie toegang toegestaan word.

Personeel moet nie probeer om die fisiese sekerheidsmeganismes (draaihekke & valdeure), of elektroniese (logiese) sekerheidsmaatreëls te omseil nie.

Die fisiese sekerheidstappe wat geneem word, is die eerste linie van verdediging teen ongemagtigde toegang tot die Munisipaliteit se inligtingsbates.

## VIRUSBESKERMING

Die IT-funksie moet altyd toesien dat rekenaars met 'n goedgekeurde anti-viruspakket toegerus is.

Kontroleer verwyderbare media vir virusse (stiffies, USB Toestelle en CDROMS) voor dit oopgemaak word en op die rekenaar gestoor word (die anti-virusprogrammatuur moet ingestel word om die taak outomaties te doen).

Lei gebruikers op om nie e-pos wat verdag voorkom, oop te maak nie. Bevestig altyd of die e-pos van ’n betroubare bron gestuur is indien daar onsekerheid oor die inhoud bestaan.

Gebruikers moet by die IT-afdeling seker maak voor e-pos oor nuwe virusse aan kollegas aangestuur word. In baie gevalle is dit ’n vals alarm met die doel om paniek te veroorsaak en sodoende die netwerk met onnodige boodskappe te oorlaai.

Wanneer daar van personeel verwag word om hul persoonlike tuisrekenaars vir amptelike Munisipale pligte te gebruik, moet die rekenaar ’n anti-virusprogram geïnstalleer hê. Die program moet gereeld bygewerk word om te verseker dat voorsiening vir die nuutste virusse gemaak is.

## REKENINGBELEID

### WAGWOORD

**Verpligte wagwoordverandering** – Die stelsel sal twaalf (12) wagwoorde onthou. Dit sal verhoed dat die gebruiker dieselfde wagwoord herhaaldelik gebruik. Indien ’n gebruiker sy/haar wagwoord vergeet, moet die stelseladministrateur gekontak word.

**Maksimum vervaltyd van wagwoord** - Dertig (30) dae, waarna die gebruiker ’n nuwe wagwoord moet insleutel en bevestig.

**Minimum wagwoordlengte -** Sewe (7) karakters wat minstens een hoofletter alfabetletter, een kleinletter alfabetletter en een syfer moet insluit. Spesiale karakters word ook toegelaat, maar is opsioneel.

### GEBRUIKERREKENINGWEIERINGBELEID

**Rekeningweieringsgrens** – Drie (3) ongeldige aantekenpogings sal toegelaat word waarna die gebruikerrekening geweier sal word. Om die rekening te herstel, moet die stelseladministrateur gekontak word.

**Duur van rekeningweiering** - Permanent. Die netwerkadministrateur moet gekontak word om die rekening te herstel.

## ALGEMEEN

**Dwing gebruikeraantekenbeperkings af (Enforce user logon restrictions** ) – Aan. Gekoppel aan rekeningaantekenure.

**Maksimum toleransie vir rekenaarhorlosie-sinkronisering (Maximum tolerance for computer clock synchronization)** – Vyf (5) minute

## PLAASLIKE BELEIDE

### OUDITBELEID

**Oudit rekening-aantekenpogings**- Rekord word gehou van suksesvolle en mislukte pogings om op die netwerk aan te teken.

**Oudit rekeningbestuur** – Suksesse en mislukkings word daagliks gemonitor.

**Oudit gidsdienstoegang** - Suksesse en mislukkings word daagliks gemonitor.

**Oudit aantekenpogings** - Suksesse en mislukkings word daagliks gemonitor.

**Oudit voorwerptoegang** - Suksesse en mislukkings word daagliks gemonitor.

**Oudit beleidsverandering** - Suksesse en mislukkings word daagliks gemonitor.

**Oudit voorreggebruik** - Suksesse en mislukkings word daagliks gemonitor.

**Oudit prosesnasporing** - Suksesse en mislukkings word daagliks gemonitor.

**Oudit stelselgebeure** - Suksesse en mislukkings word daagliks gemonitor.

## SEKERHEIDSOPSIES

**Teken gebruikers outomaties af na verstryking van aantekentyd** – Aantekenure is tussen 07H00 en 17H00. Na hierdie tydperk word gebruikers outomaties deur die stelsel afgeteken. Enige gebruiker wat na hierdie ure werk, moet by die IT-afdeling aansoek doen vir toestemming om sy/haar aantekenure te verander.

Moenie laaste gebruikernaam in aantekenskerm toon nie (Do not display last user name in logon screen) – Aan.

Verhoed gebruikers om drukker-aandrywers te installeer (Prevent users from installing printer drivers) – Aan.

Verhoed gebruikers om programmatuur te installeer (Prevent users from installing software) – Aan.

**WWW Rondblaaier /(browser)-toegang** - Alle rondblaaiers moet ingestel wees om toegang tot die Internet via instaanbedieners of via ’n perseel-instaanbediener te verkry, wat gekonfigureer is om toegang tot die Internet te verkry. Geen ander vorm van toegang tot werwe op die Internet word toegelaat nie. Dit sluit verbindings met alternatiewe diensverskaffers deur middel van ’n inbelmodem, gehuurde datalyn, private mikrogolfverbinding, radio-modem of enige ander vorm van toegangsmetode in. Gebruikers sal aanspreeklik gehou word vir sekerheidsbreuke, verlies van data of die ingevaarstel van inligting deur onveilige rondblaaipraktyke.

**Spermuur** – ’n Spermuur sal geïnstalleer word om die Munisipaliteit se interne netwerke en stelsels teen eksterne aanvalle en penetrasiepogings te beskerm. Die skep van ’n gedemilitariseerde sone word verkies, maar is nie verpligtend nie. Hierdie beleid kan hersien word indien die Munisipaliteit ’n hoë voorkoms van penetrasiepogings ondervind. Die spermuur moet gekonfigureer word om minstens die volgende te voorsien:

Network Address Translation (NAT)/(Netwerkadresherleier)

Proxy services /(Instaanbedieners)

Port blocking and control / (Poortblokkering en beheer)

Packet sniffers/ (Pakkie-snuffelaars)

Intrusion Detection and virus attack protection /(Indringingsopsporing en virusaanvalbeskerming)

WWW management features /(WWW bestuurseienskappe)

Logging of audit information /(Opteken van ouditinligting)

Custom rule formulation and configurations /(Pasgemaakte reëlformulering en konfigurasies)

## GEBRUIKERSBELEID

Die toegang wat deur die Munisipaliteit verskaf word, moet nie gebruik word om toegang tot enige materiaal van ’n seksuele, gewelddadige, destruktiewe of potensieel skadelike aard te verkry nie. Die stelsel moet op ’n morele en etiese wyse gebruik word.

As gevolg van stelselbeperkings, mag toegangsverbindings nie vir langer as 8 ure per dag gebruik word nie.

Tensy spesifiek gemeld, bied die Munisipaliteit geen tegniese ondersteuning vir persoonlike (tuis-) rekenaars nie.

Wagwoorde moet geheim gehou word en mag onder geen omstandighede openbaar gemaak of aan ’n ander gebruiker oorgedra word sonder om die amptelike aansoekproses te volg nie.

Daar word van gebruikers verwag om alle sekerheidsbreuke of vermeende sekerheidsbreuke by die Bestuurder van IT en hul onmiddellike Bestuurder aan te meld.

Die gebruikerrekening mag nie gebruik word om enige onwettige bedrywighede te pleeg nie. Dit is die verantwoordelikheid van Bestuur om toe te sien dat die sekerheidsbeleide doeltreffend aan gebruikers gekommunikeer word ten einde aanspreeklikheid te vestig.

Die rekenaar moet met die nuutste anti-virusagent wat deur die Munisipaliteit aanvaar word, gelaai word. Munisipale werknemers kan ’n afskrif by die IT-departement kry.

Gebruikers sal aanspreeklik gehou word vir optrede wat onder die spesifieke gebruikerprofiel geneem word.

Gebruikers mag nie hul rekenaars met ’n oop sessie onbeman laat nie. Gebruikers moet afteken, ’n wagwoordskermbewaarder (‘screen saver’) aktiveer, of die skerm sluit wanneer die rekenaar onbeman is terwyl dit nog aangeteken is.

Gebruikers moet kopiereg, handelsmerke, lisensies en verwante wetgewing respekteer.

Die diens moet gebruik word op ’n wyse wat nie met ander netwerkgebruikers, dienste en / of toerusting inmeng of dit ontwrig nie.

## WETLIKE EN REGULERENDE VEREISTES

Alhoewel die persoonlike gebruik van die Munisipaliteit se inligtingstelsels binne perke toegelaat word, word misbruik van hierdie stelsel en die gebruik van obsene, rassistiese of andersins aanstootlike stellings streng verbied.

Die Munisipaliteit moet binne die grense van statutêre wette en regulasies funksioneer en daaraan voldoen. Waar van toepassing, geld internasionale wette ook (bv. VISA / MasterCard Standaarde).

Versuim om aan hierdie beleid te voldoen sal as wangedrag beskou word en afhangende van die omstandighede en erns van die oortreding, kan dissiplinêre optrede onder andere een van die volgende vorms aanneem:

Dissiplinêre Berading

Mondelinge Waarskuwing

Skriftelike Waarskuwing

Diensbeëindiging; of

Summiere Ontslag

Die volgende algemene riglyne kan gebruik word vir doeleindes van dissiplinêre optrede teen werknemers wat hierdie beleid oortree:

| **Oortreding / Kategorie** |
|---|
| Verandering van enige konfigurasiestellings om sekerheid of enige ander beheermeganisme te omseil en sodoende die Munisipaliteit se inligtingsbates aan ongemagtigde wysiging, vernietiging, korrupsie of openbaarmaking van vertroulike inligting blootstel. |
| 'n Ander gebruiker toelaat om met jou rekeningbesonderhde en wagwoord toegang tot die Munisipaliteit se netwerk te verkry. |
| Die rekening van 'n ander gebruiker te gebruik om ongemagtigde toegang tot data, lêers of netwerkdienste te verkry. |
| Enige poging aanwend om sekerheidsmeganismes of -prosesse te beproef of te omseil. |
| Misbruik van spesifieke hulpbronne of dienste bv. e-pos of internet. |
| Verlies van die Munisipaliteit se bates bv. draagbare rekenaars as gevolg van nalatigheid (bv. diefstal uit 'n motor wat sonder toesig gelaat is met waardevolle Munisipale bates in die motor). |

| Oortreding / Kategorie |
| --- |
| Infeksie van die Munisipaliteit se netwerk met virusse deur na te laat om die voorgeskrewe anti-virusagent te installeer en by te werk of dit van die afstandrekenaar te verwyder. |
| Versuim om ongemagtigde afwykings van beleid / standaarde of sekerheidsinsidente aan te meld. |
| Laai van onwettige programmatuur en die gevolglike infektering van die Munisipaliteit se rekenaar met virusse of Trojaanse perde. |
| Versuim om die amptelike anti-virusproduk op persoonlike rekenaars en draagbare rekenaars te gebruik. |
| Doelbewuste aflaai en / of oopmaak van virus-geïnfekteerde lêers. |
| Buitewerkingstelling, verwydering van installering of wysiging van die oorspronklike konfigurasie van die Munisipaliteit se anti-virusproduk, tensy spesifiek gemagtig om dit te doen. |
| Die konfigurasie en gebruik van onbekragtigde deelware. |

| Onderwerp | Kanaal / Optrede |
|---|---|
| Bo-na-onder-kommunikasie | Kommunikasie van Beleid deur lede van die Inligtingstegnologie Loodskomitee (ITCSC) aan Bestuurders van alle Munisipale Departemente en derde partye. |
| Bewusmaking | Publisering op Intranet en Elektroniese Kennisgewingbordstelsel (indien beskikbaar).<br><br>Stel elektroniese aanbieding op met sekerheids- en bedryfsvereistes vir gebruikers.<br><br>Versoek nuwe en bestaande gebruikers om ontvangs van Beleid te erken en Aanvaarding van IT-beleidsvoorwaardes te onderteken. |
| Bestuurskwessies | Bepaal huidige voldoening aan Beleid en omskryf gapings.<br><br>Omskryf plan van aksie om in ooreenstemming met Beleid te kom.<br><br>Maak lys van residuele risiko's en Bestuursplanne.<br><br>Hersien inbelverbindingsprosesse en werk dit by.<br><br>Voortdurende monitering van voldoening.<br><br>Gereelde hersiening en verspreiding van beleid. |

# NETWERKSEKERHEIDBELEID

## DOEL

Die doel van hierdie Beleid is om ’n vaste fondament te voorsien vir die ontwikkeling, implementering en instandhouding van veilige praktyk in ***KAAP AGULHAS*** Munisipaliteit se netwerkomgewing.

## AGTERGROND

Netwerksekerheid behels die beskerming van die Munisipaliteit teen die bedreigings wat gemagtigde en ongemagtigde netwerkaktiwiteit inhou. Die bedreigings neem toe as gevolg van die onderlinge verbinding van netwerke en die samekoms van verskillende netwerkdienste (stem, data ens.) wat dit moeilik maak om grense rondom die Munisipaliteit af te baken en beheer uit te oefen vir die beskerming van interne bates.

Onbewustheid van die risiko dat eksterne verbindings die gevaar van ’n sekerheidsbreuk kan verhoog, hou opsigself ’n risiko in. Netwerkverbindings moet dus beskerm word op ’n vlak wat met die risiko ooreenstem. Daar moet aanvaar word dat verbindingspartye tot ’n sekere mate vyandig is en streng beheer moet word om te verseker dat die toegang waarvoor die verbinding ooreengekom is, gehandhaaf word.

## BESTEK

Hierdie Beleid is van toepassing op alle netwerkadministrateurs, tegniese en instandhoudingspersoneel, ontwerpers en die eienaar van die Munisipaliteit se netwerk. Die netwerksekerheidsbeleid word as deel van die Munisipaliteit se IT-beleid beskou.

# TERMINOLOGIE

Die volgende terminologie geld vir die doeleindes van hierdie Beleid:

**Inligtingsekerheid.** Inligtingsekerheid omvat die Bestuursprosesse, tegnologie en versekeringsmeganismes wat die Munisipaliteit in staat sal stel om hulle transaksies te vertrou, te verseker dat die inligting stabiel is en onklaarraking as gevolg van foute, doelbewuste aanvalle of rampe toepaslik kan weerstaan en daarvan kan herstel; en dat vertroulike inligting weerhou word van diegene wat nie toegang daartoe behoort te hê nie.

**Netwerksekerheid.** Die beskerming van netwerke en hulle dienste teen ongemagtigde wysiging, vernietiging of openbaarmaking en die bied van versekering dat die netwerk sy kritiese funksies korrek uitvoer.

**Netwerktoestel.** Enige inligtingstegnologie- en kommunikasietoestel wat gebruik word om die infrastruktuur wat vir kommunikasiedienste (bedieners, roeteerders, skakelaars, brûe, spermure, enkripteringstoestelle) vereis word, te vorm.

**Gedemilitariseerde Sone (DMZ).** Die voorste linie in die beskerming van waardevolle inligtingsbates teen direkte blootstelling aan 'n onveilige omgewing of 'n netwerk wat tussen 'n beskermde netwerk en 'n eksterne netwerk ingevoeg word om 'n addisionele laag van sekerheid te verskaf.

**Sensitiewe inligting.** Enige inligting wat , indien dit sonder die toepaslike magtiging openbaar gemaak sou word, die Munisipaliteit se sekerheid of sake-inisiatiewe in gedrang sou bring.

**Netwerksnuffel**. Die gebruik van apparatuur en / of programmatuurmeganismes om elektroniese kommunikasie (verkeer) oor 'n netwerk te ontleed / te monitor.

**Operasionele omgewing.** Die omgewing wat verantwoordelik is vir die implementering en instandhouding van die daaglikse sekerheidsbedrywighede.

**Kommunikasiedraer**. Die infrastruktuur wat deur 'n diensverskaffer (bv. TELKOM) voorsien word om kommunikasietoestelle met mekaar te verbind.

**Rekenaarnetwerk.** 'n Reeks rekenaars wat met mekaar verbind is deur middel van kommunikasiedraers.

**Dataverkeer.** Inligting in elektroniese formaat wat oor 'n kommunikasiedraer gekommunikeer word.

**Toegang.** Fisiese of logiese toegang tot inligting of inligtingstelsels deur 'n reeks netwerktoestelle.

# BELEID

## ALGEMENE BELEIDSVEREISTE

Dit is die Munisipaliteit se beleid om ongemagtigde toegang, openbaarmaking, duplisering, wysiging, omleiding, vernietiging, verlies, misbruik of diefstal van inligting te verbied. Bekragtiging, toegangsbeheer, privaatheid (vertroulikheid) integriteit, beskikbaarheid en ouditstawing is die minimum sekerheidsvereistes om op die Munisipaliteit se netwerk geïmplementeer te word.

## BEKRAGTIGING

Alle netwerktoestelle, bestuurstasies en netwerkgebruike / -administrateurs moet oor unieke identifisering ooreenkomstig 'n omskrewe naamgewingskonvensie beskik. Wagwoorde moet ooreenkomstig die Munisipaliteit se wagwoordstandaarde geïmplementeer word.

## LOGIESE TOEGANGSBEHEER

Toegangbeheermeganismes moet op al die netwerktoestelle en bestuurstelsels geïmplementeer word. Toegang mag slegs in lyn met die posverantwoordelikhede van Netwerkadministrateurs toegeken word (gegrond op die noodsaaklike kennisbeginsel) toegeken word. Eksterne toegang tot

netwerktoestelle en Bestuurstelsels moet tot die minimum beperk word en waar van toepassing, moet streng beheermeganismes geïmplementeer word.

## PRIVAATHEID / VERTROULIKHEID

Alle redelike maatreëls moet getref word om te verseker dat interne en eksterne kommunikasie tussen netwerke en netwerktoestelle asook kliëntverbindings, nie sekerheid in gedrang sal bring nie. Waar van toepassing, moet enkripteringsmeganismes geïmplementeer word.

## INTEGRITEIT

Meganismes / prosedures moet in plek wees om die integriteit van alle netwerktoestelle en -verkeer te verseker. Intydse waarskuwings moet genereer word vir all konfigurasie- / toestemmingsveranderinge wat tot 'n sekerheidsbreuk kan lei.

## OUDITSTAWING / AANSPREEKLIKHEID

Ouditinligting, insluitend waarskuwings wat gegenereer word vir mislukte aantekenpogings, moet vir alle netwerktoestelle en bestuurstelsels beskikbaar wees.

## BESKIKBAARHEID

Netwerk(e) en netwerkdienste moet beskikbaar wees wanneer nodig en moet die vermoë hê om die netwerkverkeervereistes te kan hanteer.

# NETWERKBESTUUR

Die Bestuurder wat vir Inligtingstegnologie verantwoordelik is, moet oorhoofse verantwoordelikheid vir netwerkaktiwiteite toewys en 'n netwerkeienaar aanstel. Dit is die netwerkeienaar se verantwoordelikheid om onder andere voldoening aan hierdie Beleid te verseker en maandelikse terugvoering ten opsigte van die stand van voldoening te voorsien as deel van die Munisipaliteit se inligtingsekerheidsrisikobestuursproses. Die Netwerkadministrateur vervul hierdie rol.

Netwerkstrategie, standaarde, beginsels, riglyne, argitektuur, prosedures, ontwerp, konfigurasie, toerusting, programmatuur, inventarisse en kabelinligting moet formeel gedokumenteer word, bygewerk word en jaarliks hersien word. Slegs gemagtigde personeel mag toegang tot hierdie inligting / dokumentasie toegelaat word ooreenkomstig die sensitiwiteit / sekerheidsklassifikasie.

Menslike hulpbronne en infrastruktuur wat krities is tot die kontinuïteit van netwerkdienste moet geïdentifiseer word en enkelpunte van onderbreking moet geminimaliseer word.

Alle eksterne verbindings met die Munisipaliteit se netwerk moet deur ’n risiko-ontleding voorafgegaan word en minstens deur ’n spermuur of soortgelyke soort toestel beskerm word. Nie-IP netwerkverbindings moet deur definisiekenmerke en / of spesifieke konfigurasies beveilig word om toegangvermoëns te beperk en aan die sekerheidsvereistes te voldoen. Die verbindings moet periodiek hersien word deur middel van ’n naspoorbare proses. Waar toepaslik, moet interne netwerke (d.i. Plaaslike Areanetwerke /LAN’s) waar sensitiewe inligting verwerk word, ook ooreenkomstig die sensitiwiteit van die inligting beskerm word.

Alle eksterne verbindings / derde partye tot die netwerk moet toegewys word aan ’n eienaar wat deur die netwerkeienaar en die hoof van die sake-eenheid wat indiwidueel geïdentifiseer en gestaaf moet word, goedgekeur word. (Verwys asseblief na die volledige beleid oor derdepartyverbindings).

Ten einde ’n duidelike beeld van die netwerk te bekom en ongewenste verbindings te minimaliseer, moet netwerktoegangsbeheer sentraal deur die netwerkeienaar of ’n verantwoordelike persoon wat deur hom/haar aangestel is, goedgekeur word.

Die Munisipaliteit se netwerk moet verkieslik beskerm word deur die skep van ’n gedemilitariseerde sone (DMZ). Geen sensitiewe inligting mag in die DMZ gestoor word nie.

Dienste wat van interne of eksterne diensverskaffers verkry word, moet in formele ooreenkomste omskryf word. Die ooreenkomste moet die vereistes vir sekerheidskontroles spesifiseer. Meganismes moet in plek wees om nakoming van hierdie vereistes te meet.

Slegs netwerkdienste wat spesifiek vir sakedoeleindes vereis word, word toegelaat en alle onnodige netwerkdienste moet versper (‘disabled’) word.

Formele opstellingstandaarde moet ooreengekom word en geen netwerktoestel mag in die operasionele omgewing ontplooi word met verstek- (default) fabriekswagwoordstellings of enige ander konfigurasie wat ’n bedreiging vir sekerheid inhou nie, byvoorbeeld oop lêeroorplasingprotokol (FTP) poorte of uitsaaikonfigurasie-inligting oor die netwerk.

Formele prosesse moet geïmplementeer word om te verseker dat alle toepaslike sekerheidsregstellings bygewerk word.

Metodes en prosedures moet geïmplementeer word waardeur netwerksekerheidskwessies op ’n konsekwente manier hanteer word. Die uitkoms moet op rekord gehou word vir toekomstige verwysing.

## VERKEERSBESTUUR

Netwerktoestelle moet gekonfigureer word om ongemagtigde toegang te voorkom. Die konfigurasie(s) moet minstens jaarliks hersien of na omvattende veranderinge word en die

gesondheid moet minstens kwartaalliks gekontroleer word. Ongemagtigde veranderinge moet as ’n sekerheidsbreuk hanteer word.

Met die uitsondering van voorafgoedgekeurde operasionele netwerksnuffel- of moniteringtoestelle, mag geen ander netwerksnuffel- of moniteringstoestelle geïnstalleer word sonder die uitdruklike magtiging van die IT-bestuurder nie.

Maatreëls moet geïmplementeer word om te verseker dat die netwerkfiltreringstoestelle nie omseil kan word nie en dat toegang slegs vanaf aangewese werkstasies of gespesifiseerde IP-adresse verkry kan word deur gemagtigde veilige kanale (byvoorbeeld SSL).

Openbaarmaking / verspreiding van inligting oor die netwerk moet tot die absolute minimum beperk word.

Verkeersvloei oor die netwerk moet dieselfde beskerming-/ sekerheidseienskappe ontvang as wanneer dit ooreenkomstig die klassifiserings van die inligting gestoor word.

## NETWERKOPERASIES

Diensvlakke tussen diensverskaffers en die Munisipaliteit moet ooreengekom word en formeel gemoniteer word om ’n aanvaarbare vlak van diens te verseker. Alle ongewone inskrywings / aktiwiteite moet ondersoek word en by die toepaslike lynbestuur aangemeld word vir regstelling.

Voorafgemagtigde indringingsopsporingsmeganismes moet aangewend word as beskerming teen moontlike aanvalle (afhangende van die begroting en beskikbaarheid van tegniese vaardighede).

Doeltreffende insidentreaksie-, sakekontinuïteit- en rampherstelbeplanningsprosesse moet geïmplementeer word.

Netwerkveranderinge moet gedokumenteer word, formeel deur die netwerkeienaar aanvaar word en ’n aanvaarde IT-veranderingsbestuurbeleid en -standaard volg.

Fisiese toegang tot netwerktoestelle moet tot gemagtigde personeel beperk word. Diensverskaffers en / of kontrakteurs sonder ’n diensrekord/-geskiedenis moet onder konstante toesig wees wanneer hulle toegang tot beperkte areas verkry.

Om die risiko van onderskepping van data in transit te verminder, moet spesiale sorg geneem word om netwerkkabels teen peutery of ontwrigting te beskerm.

Rugsteunweergawes van noodsaaklike netwerkinligting en programmatuur (insluitend kommunikasie-programmatuur en funksies, netwerkbeheertabelle /-stellings, konfigurasiediagramme en inventarisse en toestelkonfigurasies) moet geneem word teen intervalle wat vereis word vir die voortgesette beskikbaarheid van die netwerk. Die rugsteunkopieë moet beskerm word teen verlies, skade en ongemagtigde toegang deur dit in ’n brandbestande kluis op die perseel te hou en afskrifte daarvan weg van die perseel.

Afstandinstandhouding moet beheer word deur toegangsregte te beperk en alle aktiwiteite aan te teken. Diagnostiese poorte op netwerktoerusting moet deur toegangkontroles beskerm word.

Toegang tot netwerktoestelle wat primêr vir sekerheidsdienste gebruik word, moet deur die Bestuurder vir Sekerheidsdienste goedgekeur word. Toegang tot enige ander netwerktoestelle moet deur 'n formele proses om toegang te versoek en te magtig, gereguleer word. Rekord moet gehou word van die gemagtigde toegang en 'n proses moet geïmplementeer word om die tydige terugtrekking van toegang wat verval het, te verseker. Die kontroles moet in die vorm van formele en naspoorbare prosesse wees.

Interne of eksterne afstandinstandhoudingsessies aan toestelle wat die sekerheidskans vorm (die serkheidsvoorwerpe wat vir beskerming gebruik word) mag nie toegelaat word nie, tensy dit deur 'n veilige kanaal (bv. SSL vir Telnet) beskerm / beheer word.

Geen modems mag aan die netwerk gekoppel word sonder die voorafgoedkeuring van die aansoeker se Bestuurder en die Bestuurders verantwoordelik vir IT-sekerheid nie. Die IT-departement moet 'n register van alle goedgekeurde modems byhou.

Geen gebruikers mag deur middel van 'n modem aan 'n ander netwerk gekoppel wees terwyl hy/sy terselfdertyd aan die Munisipaliteit se netwerk gekoppel is nie.

## RISIKOBESTUUR

'n Formele risiko-ontleding moet minstens jaarliks uitgevoer word vir netwerke wat kritiese saketoepassings ondersteun. Die resultate van risiko-ontleding moet 'n duidelike aanduiding gee van sleutelrisiko's, 'n assessering van hul potensiële sake-impak en aanbevelings vir die optrede wat vereis word om risiko tot 'n aanvaarbare vlak te verlaag.

Die sekerheidstatus van die netwerk moet onderhewig wees aan deeglike, onafhanklike en gereelde sekerheidsoudit/-oorsig. Ooreengekome aanbevelings van sekerheidsoudits / oorsigte moet geïmplementeer word en aan topbestuur gerapporteer word.

Met die uitsondering van Interne Oudit, mag geen ongemagtigde of klandestiene oudit of risiko-ontleding uitgevoer word sonder die voorafgoedkeuring van die netwerkeienaar nie.

'n Risiko-ontleding moet uitgevoer word en die resultate formeel oorweeg word voor die implementering van tegnologie wat die sekerheid van die netwerk kan benadeel. (Die instel van draadlose netwerke dien as voorbeeld.)

'n Proses moet geïmplementeer word om voldoening aan nuwe en bestaande plaaslike en internasionale statutêre vereistes te verseker.

## AANMELDING

Tensy spesifiek en formeel deur die IT-bestuurder goedgekeur, is enige afwyking van hierdie Beleid streng verbode.

## OPSOMMING VAN HOOFVERANTWOORDELIKHEDE

Hieronder volg ’n opsomming van die hoofverantwoordelikhede soos in die beleidsdokument vervat:

| Verantwoordelikheid | Eienaar | | | |
|---|---|---|---|---|
| | IT Bestuurder | Netwerk-administrateur | Bestuurders van ander Munisipale Departemente | Menslike Hulpbronne |
| Formuleer Netwerkstrategie | ✓ | | | |
| Implementering van Beleid | ✓ | ✓ | ✓ | ✓ |
| Bewusmaking | ✓ | | ✓ | |
| Beleidsbywerking / -hersiening | ✓ | ✓ | | |
| Voldoeningsmonitering | ✓ | ✓ | ✓ | |
| Moniteringsverslae | ✓ | ✓ | | |
| Bestuursinligting | ✓ | ✓ | | |
| Rapportering van Sekerheidsinsidente | ✓ | ✓ | ✓ | ✓ |
| Formulering van Operasionele Prosesse | ✓ | ✓ | | |
| Formulering van Tegniese Netwerkstandaarde | ✓ | ✓ | | |
| Risiko-ontleding | ✓ | ✓ | | |

| Verantwoordelikheid | Eienaar | | | |
|---|---|---|---|---|
| | IT Bestuurder | Netwerk-administrateur | Bestuurders van ander Munisipale Departemente | Menslike Hulpbronne |
| Gesentraliseerde Toegangsbeheer | ✓ | | | |
| Netwerkinventaris | ✓ | ✓ | | |
| Netwerksekerheidstoestelbestuur | ✓ | ✓ | | |
| Goedkeuring van Derdepartyverbindings | ✓ | | | |
| Netwerkgebeurlikheidsbeplanning (ingesluitend rampherstel) | ✓ | ✓ | | |
| Voldoeningsoorsigte uit 'n bestuursperspektief | ✓ | | ✓ | |
| Onafhanklike ad hoc oorsig | ✓ | ✓ | | |

## DISSIPLINÊRE PRAKTYKKODE

Die Munisipaliteit beskou die implementering van hierdie Beleid in 'n ernstige lig en sal nie huiwer om teen oortreders op te tree nie. Nie-voldoening aan hierdie Beleid is gronde vir dissiplinêre optrede tot en insluitende summiere ontslag.

# INTERNET-, INTRANET-, EKSTRANET- EN E-POSBELEID

## VOORWOORD

Die groei van die Internet en e-pos as primêre kommunikasiekanaal neem elke jaar toe. Die Internet en e-pos bied toegang tot inligting en dienste wat voorheen moeilik sou wees om te bekom. Daarbenewens moedig Nasionale en Provinsiale Regering die gebruik van die Internet as ’n manier om die toeganklikheid van regeringsdienste vir almal te verbeter, aan.

Toegang tot die Internet en e-pos aan organisasies en werknemers in die normale loop van hul daaglikse pligte, verhoog die risiko’s vir organisasies op vele vlakke. Die sekerheid van die Munisipale stelsels en inligting moet te alle beveilig word. Die Internet verhoog die risiko van sekerheidsbreuke, diefstal van vertroulike inligting en toevallige of doelbewuste openbaarmaking van vertroulike inligting, wat regstappe deur die gegriefde party tot gevolg kan hê.

Net soos telefone kommunikasie verbeter het, maar onderhewig was aan wydverspreide misbruik deur werknemers, so ook is die Internet en e-pos onderhewig aan misbruik. Die prys van sodanige misbruik, naamlik die koste en ook verlies aan produktiwiteit moet deur die Munisipaliteit gedra word. Die bedoeling van ’n E-posbeleid is om riglyne te voorsien vir

die gebruik van die elektroniese media en waar misbruik voorkom, word die strafmaatreëls wat teen ’n werknemer geneem kan word, uiteengesit. Die Internet- en E-posbeleid beheer ook die inhoud waartoe toegang oor die Internet verkry kan word en verbied die versending van teisterende en seksueel eksplisiete materiaal.

Die Internet- en E-posbeleid spesifiseer ook die sekerheidsmaatreëls en veiligheidsmaatreëls wat deur beide die IT-departement en die werknemer toegepas moet word.

## ALGEMENE DEFINISIES EN BETEKENIS VAN TERME

Die term “Munisipaliteit” sluit die ***KAAP AGULHAS*** Munisipaliteit met al sy Departemente in.

Die groepterm “Internet” sluit Internet, Ekstranet, Intranet en E-posdienste in. Waar ’n spesifieke woord, soos e-pos gebruik word, word dit ter opklaring gebruik en sluit dit nie noodwendig die ander in die groep uit nie.

## BELEIDSDOELWITTE

Hierdie Beleid:

Bevat die Munisipaliteit se vereistes en standaarde rakende die implementering, gebruik, bestuur en administrasie van Internettoegang.

Baken die rolle en verantwoordelikhede van deelnemende organisatoriese eenhede af.

Bevorder bewusmaking onder die Munisipaliteit se Internetgebruikers rakende die prosedures, koste en risiko’s verbonde aan verkryging van toegang tot die Internet.

Stel die Munisipaliteit se standpunt in die geval van nie-voldoening aan die Internetbeleid deur enige Munisipaliteit se Internetgebruiker.

Omskryf riglyne, standaarde en prosedures vir die Munisipaliteit se afdelings wat inligting en dienste op die Internet verskaf.

## BESTEK VAN BELEID

Die bestek van hierdie Beleid word bepaal deur die beheerde en veilige gebruik van die Munisipaliteit se infrastruktuur en Internetkanale wat deur die Munisipaliteit en sy kliënte voorsien word en sluit die volgende in:

### INTERNET

Die Munisipaliteit se Internet word gebruik as ’n addisionele leweringskanaal om kommunikasie en inligting aan die Munisipaliteit se inwoners en potensiële inwoners en werkverwante Wêreldwye Web (www) toegang aan die Munisipaliteit se werknemers te voorsien.

### INTRANET

Die Munisipaliteit se Intranet is toegewy aan die Munisipaliteit se Departemente en/of sake-eenhede om interne kommunikasie meer doeltreffend en effektief te maak.

### EKSTRANET (GESPESIALISEERDE DIREKTE VERBINDINGS)

Die Munisipaliteit Ekstranet, of uitgebreide Internet, word deur die Munisipaliteit gebruik om ’n hegte elektroniesekommunikasiekanaalverhouding met sy regeringstrukture of die privaat sektor te vorm in die geval van e-verkryging en e-regeringsbestuur.

### E-POS

Die E-posdiens wat deur die Munisipaliteit voorsien word, is gemik op meer doeltreffende en effektiewe eksterne en interne werkverwante kommunikasie. Beide intern- en ekstern-gebaseerde rondblaaiers ( byvoorbeeld “Hotmail.com”) en kliënt (byvoorbeeld “Microsoft Outlook”), e-pos, indien toegang daartoe verkry word deur die infrastruktuur en Internetkanale wat deur die Munisipaliteit voorsien word, word as onderhewig aan hierdie Beleid geag.

## EIENAARSKAP

***KAAP AGULHAS*** Munisipaliteit se Raad en Inligtingstegnologie (IT) is die eienaar van die beleid.

***KAAP AGULHAS*** Munisipaliteit Inligtingstegnologie (IT), of die Departement verantwoordelik vir IT, moet die instandhouding van die Beleid in oorleg met toepaslike partye soos van tyd tot tyd deur die Raad gemandateer uitvoer en koördineer.

## IMPLEMENTERING

Die Bestuur van die Munisipaliteit is verantwoordelik vir die implementering van die Beleid in hul eie Departemente. IT en Menslike Hulpbronne moet die implementering daarvan fasiliteer en koördineer.

Die Bestuur van die Munisipaliteit soos hieronder aangedui, is verantwoordelik vir die opstel van strategieë, subbeleide en standaarde ter ondersteuning van hierdie Beleid.

Regsdepartement: Regsriglyne / -standaarde.

IT: Apparatuur / programmatuur-argitektuur en standaarde vir Internettoegang, prosedure vir versoeke om Internettoegang en die verwerking daarvan, Internetinligtingsbeskerming, Sekerheidstandaarde en infrastruktuur, Uitkontrakteringsorosedures (indien toegepas en geïmplementeer).

Enige subbeleide/addendums moet van die Munisipaliteit se beleide afgelei word en die Munisipaliteit se oorhoofse Internetfilosofie ondersteun. Sodanige subbeleide/addendums moet deur die Raad goedgekeur word, selfs al blyk dit dat hierdie addisionele dokumente met die Munisipaliteit se Beleid ooreenstem.

# ROLSPELERS

Die hoofrolspelers ten opsigte van die ***KAAP AGULHAS*** Munisipaliteit se Internetkanale is:

***KAAP AGULHAS*** Munisipaliteit Inligtingstegnologie- en Kommunikasieloodskomitee (ITCSC).

***KAAP AGULHAS*** Munisipaliteit Inligtingstegnologie- (IT) bestuur.

***KAAP AGULHAS*** Munisipaliteit Menslike Hulpbronne (MH).

Die verantwoordelikhede van elke rolspeler in die totale risikobestuursproses van ***KAAP AGULHAS*** Munisipaliteit se Internetkanale is as volg:

## INLIGTINGSTEGNOLOGIE- EN KOMMUNIKASIELOODSKOMITEE (ITCSC):

Sien toe dat daar 'n ***KAAP AGULHAS*** Munisipaliteit IT-beleid bestaan.

Hersien die IT-beleid.

Aanbeveling van die Beleid aan die Raad.

Verkryging van Raadsgoedkeuring vir die Beleid.

## INLIGTINGSTEGNOLOGIE- (IT) BESTUUR:

Sien toe dat voldoende en kostedoeltreffende bestuur en beheerstrukture bestaan vir die behoorlike gebruik van die Munisipaliteit se IT-dienste.

Opstel en implementering van beleide en prosedures om risiko rakende die Internet doeltreffend te bestuur.

Vervul hul toegewese verantwoordelikhede soos in die IT-beleid vervat.

## MENSLIKE HULPBRONNE (MH):

Bystand met implementering van die Beleid.

Implementeer, waar nodig, dissiplinêre optrede soos in die Beleid omskryf.

# BELEIDSVERKLARINGS

Die volgende behels die kern van die Internet/Ekstranet/Intranet-beleid en sal deur spesifieke, gedetailleerde standaarde en / of prosedures wat deur die Beleidsrolspelers omskryf is, ondersteun word.

Die Internethulpbronne wat in die werkplek voorsien word, bly ten alle tye die eiendom van die Munisipaliteit.

Die hulpbronne wat voorsien word, is bedoel om spesifiek vir die werknemer se werk en werkverwante aktiwiteite gebruik te word.

Toevallige persoonlike gebruik word toegelaat mits dit:

(a) nie meer as ’n geringe hoeveelheid hulpbronne gebruik nie,

(b) nie met die werknemers se produktiwiteit inmeng nie,

(c) geen sake-aktiwiteit vooruitloop nie en

(d) nie die bedoeling van hierdie Beleid uitsluit nie.

Die Munisipaliteit behou die reg voor om enige elektroniese posboodskap en aanhangsel te lees indien dit van mening is dat die situasie dit regverdig. Die werknemer moet geen verwagting van privaatheid koester ten opsigte van inligting wat op ’n hulpbron wat deur die Munisipaliteit voorsien is, versend en / of gestoor word nie. Deur ondertekening van die Internet/E-pos-aansoekvorm, doen die werknemer afstand van enige reg om die bepalings van die Wet op die Verbod op Onderskepping en Monitering, Wet 127 van 1992.

## ONAANVAARBARE GEBRUIKE VAN DIE INTERNET EN KAAP AGULHAS MUNISIPALITEIT E-POS:

Die Munisipaliteit se e-pos- en Internettoegang mag nie gebruik word vir versending, verkryging of stoor van enige kommunikasie van ’n diskriminerende of teisterende aard of materiaal wat obseen of pornografies is nie. Die versending van boodskappe / lêers wat ras- of seksueel-teisterend van aard is, is ook verbode. Geen beledigende taal of skel- of vloektaal mag deur middel van die Munisipaliteit se e-pos of Internetstelsel, insluitend enige boodskapstelsel soos Winpop, Instant Messenger (of enige ander boodskapstelsels) versend word nie.

Elektroniese media mag nie gebruik word vir enige ander doel wat onwettig is of teen die Munisipaliteit se Beleid indruis of teenstrydig is met die Munisipaliteit se beste belang nie. Werwing van nie-Munisipale sake of enige gebruik van die Munisipaliteit se e-pos of Internet vir persoonlik gewin is verbode. Die gebruik van e-pos om aan politieke aktiwiteite deel te neem, politieke steun te werf of politieke sienswyses te ondersteun of te propageer, is verbode.

Materiaal waarop kopiereg van toepassing is wat aan entiteite anders as die Munisipaliteit behoort, mag nie deur werknemers op die Munisipaliteit se e-pos-/Internetstelsel versend word nie. Alle werknemers wat toegang tot ander maatskappye of indiwidue se materiale verkry moet alle kopiereg respekteer en mag nie materiaal waarop kopiereg van toepassing is kopieer, verkry, verander of aanstuur sonder die skriftelike toestemming van die kopiereghouer nie, of as ’n enkele afskrif vir verwysing-/rugsteundoeleindes alleenlik.

## AANVAARBARE GEBRUIKE VAN DIE INTERNET EN E-POS:

Elke personeellid het ’n verantwoordelikheid om die Munisipaliteit se beeld te handhaaf en te bevorder en om e-pos en toegang tot die Internet op ’n verantwoordelike manier te gebruik (Net-etiket).

Internettoegang word slegs vir sakedoeleindes voorsien. Internetgebruikers het ’n verantwoordelikheid om die Internet toepaslik in die uitvoering van die Munisipaliteit se sake te gebruik.

Elke werknemer is verantwoordelik vir die inhoud van alle teks, oudio of beelde wat hulle op die Munisipaliteit se e-pos/Internetstelsel plaas of versend. Geen e-pos of ander elektroniese kommunikasie mag versend word wat die identiteit van die afsender wegsteek of die afsender as iemand anders of iemand van ’n ander maatskappy of Munisipaliteit voorstel nie.

Alle boodskappe wat via die Munisipaliteit se e-pos-/Internetstelsel versend word, moet die werknemer se naam bevat.

Enige boodskappe of inligting wat deur ’n werknemer na ’n ander indiwidu buite die Munisipaliteit via ’n elektroniese netwerk (bv. elektroniese kennisgewingbord, aanlynbediener of Internet) versend word, is stellings wat die Munisipaliteit se beeld raak.

Alle uitgaande e-pos moet die ***KAAP AGULHAS*** Munisipaliteit standaard vrywaring (‘disclaimer’) bevat (Kyk Bylae A)

Alle werknemers van die Munisipaliteit is aanspreeklik vir die uitdrukking van persoonlike of Munisipale menings op die Internet en spesifiek nuusgroepe.

## ARGITEKTUUR EN INFRASTRUKTUUR:

Die Munisipaliteit se verbindings met die Internet moet aan die heersende Tegnologie-argitektuur van die Munisipaliteit voldoen.

IT, as verteenwoordiger van die Munisipaliteit, moet ’n ooreenkoms met ’n geakkrediteerde eksterne Internetdiensverskaffer (ISP), of veelvuldige Internetdiensverskaffers aangaan indien dit in die Munisipaliteit se beste belang is, vir toegang tot die Internet. Hierdie ooreenkomste sal die enigste amptelike Munisipaliteit-goedgekeurde Internetverbindings uitmaak. Geen ander Munisipale Departement mag sy eie aparte Internettoegang onderhandel nie.

Slegs IT word toegelaat om Web-gasheerdienste te onderhandel. Alle Munisipale Internetblaaie moet by ’n  sentrale Web-gasheerbediener gehou word wat die nodige stelseloortolligheid-, sekerheids- en diensvlakooreenkomste ondersteun.

## NAKOMING

Al die Munisipaliteit se inligting en dienste op die Internet moet voldoen aan die strategie, standaarde en prosedures wat in hierdie beleid omskryf word, naamlik Internetontwerp-, implementering- en aanbiedingstandaarde; Apparatuur- / programmatuurstandaarde vir Internettoegang; Prosedure vir Versoek om Internet-/Intranettoegang; Regsriglyne en -standaarde; Internetuitkontrakteringstandaarde; Internetinligtingbeskermingstandaarde; Uitkontrakteringprosedures; Inter-/Intranet-infrastruktuur, Samewerkende Webstrategie; en Internet/Intranet/Ekstranet strategieë.

Versuim om aan die Munisipaliteit se Internet/Intranet/Ekstranet Beleid of enige van sy voorskrifte en standaarde te voldoen, sal dissiplinêre optrede tot gevolg hê.

Die Munisipaliteit behou die reg voor om enige gebruiker se Internettoegangsregte en / of toepassing te verwyder of te kanselleer indien getoon kan word dat dit in die beste belang van die Munisipaliteit is.

Die Munisipaliteit behou die reg voor om toegang tot enige kategorie of indiwiduele Internetwerf te "blokkeer" as getoon kan word dat dit in die beste belang of sakebelang van die Munisipaliteit is.

Alle materiaal op die Munisipaliteit se Internetwerf mag nie die reg van enige derde party skend, plagiariseer of inbreuk daarop maak nie, insluitend kopiereg, handelsmerk of eiendomsreg.

## SEKERHEID

Internetgebruikers moet te alle tye die huidige Internetsekerheidpraktyke in die Munisipaliteit nakom wanneer vertroulike of missie-kritiese inligting oor die Internet versend word.

Die Munisipaliteit behou die reg voor om enige werknemers se Internet/Intranetkommunikasie en gebruik te monitor. Alle boodskappe wat geskep, versend of opgeroep word via die Munisipaliteit se e-pos/Internet is die eiendom van die Munisipaliteit en sal as organisasie-inligting beskou word. Werknemers moet nie aanvaar dat elektroniese kommunikasie heeltemal privaat is nie en moet hoogs vertroulike data op ander maniere versend. Ten einde die werknemer se privaatheid te beskerm, sal niemand egter toegelaat word om toegang tot die stelsel te verkry om ander e-pos te lees sonder die voorafgoedkeuring van die Munisipaliteit se ITCSC nie. Dit bied 'n mate van versekering dat e-pos nie willekeurig gelees sal word nie.

Die voorsiening van sekerheid is belangrik en alle dienste en inligting wat op die Internet voorsien word, moet aan die nuutste Munisipaliteit Internetsekerheidstandaard voldoen ten opsigte van: bekragtiging, nie-repudiëring (van oorsprong en ontvangs) en data-integriteit en dataprivaatheid. Die IT-departement moet alle sekerheidskwessies rakende Munisipaliteit Internetaansoeke goedkeur voor implementering daarvan.

Goedkeuring van die uitkontraktering van Internetinhoudontwikkeling sal van die volgende afhang:

***KAAP AGULHAS*** Munisipaliteit se direkte goedkeuring van:

Ooreenstemming met die Munisipaliteit se Internetstrategie;

Verhouding- en steunfunksies ter voldoening aan die Munisipaliteit se Internet Kliëntediensbeleide;

Voldoening aan die Munisipaliteit se Internetstandaarde en -prosedures.

Voldoening aan die Munisipaliteit se Toepassingstandaarde vir Internetontwikkeling en optree as Internet webbedienergasheer.

Goedkeuring deur ***KAAP AGULHAS*** Munisipaliteit Tegniese Steun vir:

Tipe diens wat uitgekontrakteer word en die toekomstige integrasie daarvan met die Munisipaliteit se Internet- tegniese infrastruktuur;

Ooreenstemming met die Munisipaliteit se Internet- Inligtingsbeskerming- en Sekerheidstandaarde.

Goedkeuring deur ***KAAP AGULHAS*** Munisipaliteit se Tegniese Strategie en Argitektuur van:

Voldoening aan die Munisipaliteit se Tegniese Apparatuur- en programmatuurstrategie en -argitektuur.

Die oordrag van eienaarskap en verantwoordelikheid van die Munisipaliteit se Internet-inligting- en/of dienste sal nie toegelaat word wanneer Internet ontwikkeling uitgekontrakteer word nie. Al die Munisipaliteit se Internet-inligting sal binne die Munisipaliteit se perseel gehou word om doeltreffende bestuur en beheer daaroor te verseker. Fragmentering en duplisering van die Munisipaliteit se inligting en /of dienste deur eksterne uitgekontrakteerde verkopers sal nie toegelaat word nie.

# OORTREDINGS EN STRAFBEPALINGS

Enige werknemer wat die voorreg van Munisipaliteit-gefasiliteerde toegang tot e-pos of die Internet misbruik, sal onderhewig wees aan dissiplinêre optrede wat tot ontslag kan lei. Indien nodig behou die Munisipaliteit die reg voor om toepaslike wetsbeamptes in te lig rakende enige onwettige oortredings.

Die onderstaande algemene riglyne kan gebruik word vir die doeleindes van dissiplinêre optrede teen werknemers wat hierdie beleid oortree:

| **Oortreding / Kategorie** |
|---|
| Oplaai van onwettige programmatuur of aanstootlike, ontwrigtende, beledigende of immorele materiaal, soos pornografiese materiaal, op 'n rekenaar wat deur die Munisipaliteit besit word. |
| Versending van eksterne boodskappe sonder om die Munisipaliteit se standaard vrywaring ('disclaimer') aan te heg. |
| Die verkryging van toegang tot pornografiese, aanstootlike, immorele, beledigende, ontwrigtende of diskriminerende materiaal. |
| Verandering van die konfigurasie van enige Internetbediener, Bediener of rekenaar sonder behoorlike magtiging. |
| Gebruik van die Munisipaliteit se Internethulpbronne vir persoonlike gewin. |
| Oormatige rondblaai op die internet waar dit duidelik is dat die werwe wat besoek word nie werkverwant is nie of enigsins verband hou met die dienste wat deur die Munisipaliteit gelewer word nie. |
| Rondblaai op die internet waar sodanige rondblaaiery lei tot agteruitgang in die werknemer se prestasie en werkgehalte. |
| Openbaarmaking van Sekerheidsidentiteitsname en wagwoorde aan enige ander persoon, insluitend nie-personeellede. |
| Doelbewuste aflaai en / of oopmaak van virus-besmette lêers. |
| Versending van materiaal waarop kopiereg gehou word sonder magtiging van die kopiereghouer. |
| Verspreiding van pornografiese, aanstootlike, immorele, beledigende, ontwrigtende |

| |
|---|
| of diskriminerende materiaal. |
| Versending of aanstuur van kettingbriewe via die e-posstelsel (insluitend Powerpoint skyfies, geheuestokkies of enige ander soortgelyke formate) |
| Verkryging van toegang tot Internetbedieners sonder gemagtiging. |
| Versending van eksterne boodskappe wat persoonlike menings en / stellings bevat wat as die Munisipaliteit se mening beskou kan word. |

## ELEKTRONIESE POSSEKERHEID

### MUNISIPALE EIENDOM:

As ’n instrument om produktiwiteit te bevorder, moedig die Munisipaliteit die regmatige organisatoriese gebruik van elektroniese kommunikasie aan. Elektroniese kommunikasiestelsels, en alle boodskappe wat op elektroniese kommunikasiestelsels gegenereer word of hanteer word, insluitende rugsteunkopieë, word geag die eiendom van die Munisipaliteit te wees.

### GEMAGTIGDE GEBRUIK:

Die Munisipaliteit se elektroniese kommunikasiestelsels moet hoofsaaklik net vir Munisipale aktiwiteite gebruik word. Toevallige persoonlike gebruik is toelaatbaar op voorwaarde dat:

(a) Dit nie meer as ’n geringe hoeveelheid hulpbronne gebruik nie,

(b) dit nie met die produktiwiteit van die werknemer inmeng nie, en

(c) dit nie enige Munisipale Sakebedrywigheid vooruitloop nie.

Gebruikers word verbied om die Munisipaliteit se elektroniese kommunikasiestelsels vir liefdadigheidskwessies, privaat sakebedrywighede, pret of vermaaklikheidsdoeleindes te gebruik.

Werknemers word daaraan herinner dat die gebruik van Munisipale hulpbronne, insluitende elektroniese kommunikasie, nooit die indruk of die werklikheid van onvanpaste gebruik moet

skep nie. Toegang tot privaat e-posrekeninge word verbied omdat dit ’n bron van sekerheidsrisiko is. Privaat internetbanksake word toegelaat indien toegang tot die internet reeds ten opsigte van werksvereistes aan indiwidue toegestaan is, op voorwaarde dat bogenoemde reëls nagekom word.

## VERSTEKVOORREGTE:

Werknemervoorregte op elektroniese kommunikasiestelsels moet sodanige toegewys word dat slegs die funksies wat nodig is om ’n taak te verrig toegewys word. Hier benadering staan algemeen bekend as die konsep van “minste voorreg”. Uitsaaigeriewe (soos ’n “everyone” of “send to all” E-pos) moet slegs gebruik word nadat toestemming van ’n Departementele Bestuurder verkry is en moet deur die IT Netwerk-administrateur versend word.

## GEBRUIKER-ONDERSKEIDING:

Persoonlike gebruikeridentiteitsname en verwante wagwoorde moet gebruik word om verskillende gebruikers te identifiseer en te bekragtig en om die kommunikasie van verskillende gebruikers van mekaar te onderskei. Faksmasjiene wat nie aparte posbusse vir verskillende ontvangers het nie, hoef nie gebruiker-onderskeiding te ondersteun nie.

## GEBRUIKERAANSPREEKLIKHEID:

Ongeag die omstandighede, moet die Beleide wat op gebruikersidentiteitsname en wagwoorde in die Munisipaliteit van toepassing is, ook op toegang tot e-pos toegepas word. Versuim stel die gemagtigde gebruiker bloot aan aanspreeklikheid vir optrede wat die ander party met die wagwoord neem. Indien gebruikers rekenaardata moet deel, moet hulle boodskapaanstuurgeriewe, openbare lêergidse (“directories”) op plaaslike areanetwerkbedieners en ander gemagtigde meganismes waarop inligting gedeel kan word, gebruik.

## GEBRUIKERIDENTITEIT:

Wanvoorstelling, verduistering, onderdrukking of vervanging van ’n gebruiker se identiteit op ’n elektroniese kommunikasiestelsel is verbode. Die gebruiker se naam, elektroniese

posadres, organisatoriese affiliasie en verwante inligting wat by elektroniese boodskappe of inskrywings ingesluit word, moet die werklike opsteller van die boodskappe of inskrywings weerspieël.

## GEEN VERSTEKBESKERMING:

Werknemers word daaraan herinner dat die Munisipaliteit se Elektroniese Kommunikasiestelsels nie by verstek geënkripteer is nie. Indien sensitiewe inligting deur elektroniese kommunikasiestelsels versend moet word, moet enkripsie- of soortgelyke tegnologie toegepas word om die data te beskerm. Bystand kan by die Inligtingstegnologie Departement bekom word.

## RESPEKTERING VAN REG OP PRIVAATHEID:

Behalwe waar spesifiek andersins bepaal word, mag werknemers nie elektroniese kommunikasie onderskep of openbaar maak, of bystand verleen om dit te onderskep of openbaar te maak nie. Die Munisipaliteit is daartoe verbind om die regte van sy werknemers te respekteer, insluitende hul redelik verwagting op privaatheid. Die Munisipaliteit is ook verantwoordelik om sy elektroniese kommunikasienetwerke te diens en te beskerm. Om dit te bereik, is dit by geleentheid nodig om elektroniese kommunikasie te onderskep of openbaar te maak of bystand te verleen om dit te onderskep of openbaar te maak.

## GEEN GEWAARBORGDE PRIVAATHEID VAN BOODSKAPPE:

Die Munisipaliteit kan egter nie waarborg dat elektroniese kommunikasie privaat sal wees nie. Werknemers moet daarvan bewus wees dat elektroniese kommunikasie, afhangende van die tegnologie, deur ander aangestuur, onderskep, gedruk en gestoor kan word. Daarbenewens kan toegang tot elektroniese kommunikasie deur ander ingevolge hierdie beleid verkry word.

## GEREELDE BOODSKAPMONITERING:

Dit is die Munisipaliteit se beleid om NIE gereeld die inhoud van elektroniese kommunikasie te monitor nie. Die inhoud van elektroniese kommunikasie kan egter gemonitor word en die gebruik van elektroniese kommunikasiestelsels sal gemonitor word om operasionele,

instandhoudings-, oudit-, sekerheids- en ondersoekende bedrywighede te ondersteun. Gebruikers moet hul elektroniese kommunikasie sodanig struktureer in die wete dat die Munisipaliteit die inhoud van elektroniese kommunikasie van tyd tot tyd kan en sal ondersoek.

## STATISTIESE DATA:

In ooreenstemming met algemeen aanvaarde praktyk, versamel die Munisipaliteit statistiese data rakende elektroniese kommunikasie. Met behulp van sodanige inligting kan tegniese steunpersoneel die gebruik van elektroniese kommunikasie monitor ten einde die voortgesette beskikbaarheid en betroubaarheid van hierdie stelsels te verseker.

## TOEVALLIGE OPENBAARMAKING:

Dit mag nodig wees vir tegniese steunpersoneel om die inhoud van indiwiduele werknemers se kommunikasie in die loop van probleemoplossing na te gaan. Tegniese steunpersoneel mag nie die inhoud van ’n indiwiduele werknemer se kommunikasie uit nuuskierigheid of op versoek van indiwidue wat nie die behoorlike goedgekeurde kanale gevolg het, nagaan nie.

## INHOUD VAN BOODSKAPPE:

Werkers mag nie vloektaal of onwelvoeglike taal gebruik, of afbrekende aanmerkings in elektroniese posboodskappe maak wanneer werknemers, klante, mededingers, of ander bespreek word nie. Sodanige aanmerkings – selfs as dit as ’n grap bedoel word – kan regsprobleme soos handelslaster en karakterskending tot gevolg hê. Spesiale sorg moet geneem word omdat rugsteun- en argiefafskrifte van elektroniese boodskappe meer permanent en meer geredelik toeganklik is as tradisionele kommunikasie op papier.

## AANSTUUR VAN BOODSKAPPE:

In die wete dat sommige inligting vir spesifieke indiwidue bedoel is en dalk nie geskik is vir algemene verspreiding nie, moet elektroniese kommunikasiegebruikers omsigtigheid beoefen

wanneer boodskappe aangestuur word. Sensitiewe inligting moet aan geen party buite die Munisipaliteit aangestuur word sonder die voorafgoedkeuring van ’n Departementele Bestuurder nie. Willekeurige aanstuur van boodskappe aan partye buite die Munisipaliteit word verbied tensy die vooraftoestemming van ’n Departementele Bestuurder verkry is en dan moet die boodskap deur die IT Netwerkadministrateur versprei word.

## HANTERING VAN INLIGTING RAKENDE SEKERHEID:

Gebruikers moet spoedig alle inligtingsekerheidsalarms, waarskuwings, vermeende kwesbaarhede, ensovoorts by die IT-departement rapporteer. Gebruikers word verbied om die Munisipaliteit se stelsels te gebruik om sodanige inligting aan ander gebruikers aan te stuur, ongeag of die ander gebruikers intern of ekstern tot die Munisipaliteit is.

## OPENBARE VERTOË:

Geen media-advertensie, Internet tuisblad, elektroniese kennisgewingbordboodskap, elektroniese posboodskap, stemboodskap, of enige ander openbare vertoë oor die Munisipaliteit mag uitgereik word tensy dit eers deur die toepaslike goedkeuringskanale is nie. Toestemming moet deur die toepaslike Departementele Bestuurder verleen word, en moet dan deur die IT Netwerkadministrateur uitgereik word.

## GEBRUIKERRUGSTEUN:

Indien ’n elektroniese posboodskap inligting bevat wat toepaslik is vir die afhandeling van ’n transaksie, dit potensieel belangrike verwysingsinligting bevat, of ’n waarde het as bewys vir ’n Munisipale Bestuursbesluit, moet dit vir toekomstige verwysing behou word. Die meeste elektroniese posboodskappe val nie in hierdie kategorieë nie en kan dus na ontvangs geskrap word. Gebruikers moet gereeld belangrike inligting uit elektroniese posboodskaplêers na woordverwerkingsdokumente, databasisse en ander lêers oorplaas. Elektroniese posboodskapstelsels is nie bedoel vir die argiefbewaring van belangrike inligting nie. Belangrike gestoorde elektroniese posboodskappe kan periodiek deur stelseladministrateurs verwyder word, per abuis deur gebruikers geskrap word en andersins verlore gaan wanneer stelselprobleme voorkom.

## ARGIEFBEWARING:

Alle amptelike Munisipale elektroniese posboodskappe, insluitend die wat ’n formele bestuursgoedkeuring, magtiging, delegasie of oorhandiging van verantwoordelikheid, of soortgelyke transaksie bevat, moet in die argief bewaar word.

## VERWYDERING VAN GESTOORDE ELEKTRONIESE BOODSKAPPE:

Boodskappe wat nie meer vir sakedoeleindes benodig word nie, moet periodiek deur gebruikers van hul elektroniese boodskapstoorareas geskrap word. Na ’n sekere tydperk – gewoonlik ses maande – sal elektroniese boodskappe wat op multi-gebruikerstelsels gestoor word, outomaties deur stelseladministrasiepersoneel geskrap word. Dit sal nie slegs skaars stoorplek vermeerder nie, maar sal ook die bestuur van rekords en verwante aktiwiteite vereenvoudig.

## TEISTERENDE OF AANSTOOTLIKE MATERIAAL:

Die Munisipaliteit se rekenaar- en kommunikasiestelsels is nie bedoel om gebruik te word en moenie gebruik word, as uitoefening van die werkers se reg op vrye spraak nie. Seksuele, etniese en rassediskriminasie -- insluitend ongewenste telefoonoproepe, elektroniese pos en interne pos -- is streng verbode en is gronde vir dissiplinêre optrede. Werkers word aangemoedig om die opsteller van aanstootlike e-posboodskappe, telefoonoproepe en/of kommunikasie direk te beantwoord.

Indien die opsteller nie spoedig die versending van aanstootlike boodskappe staak nie, moet werkers die kommunikasie aan hul Bestuurder en die Departement Menslike Hulpbronne rapporteer. Die Munisipaliteit behou die erg voor om enige materiaal wat dit as aanstootlik of potensieel onwettig beskou, te verwyder.

## TOEGANG TOT INTERNET E-POS:

Toegang tot Internet-gebaseerde elektroniese pos mag slegs via die internet E-posbedieners wat deur die Munisipaliteit verskaf word verkry word, wanneer die teikenrekenaar aan die Munisipaliteit se netwerk gekoppel is.  Gebruikers word nie toegelaat om bv. uit te bel na

diensverskaffers om toegang tot e-pos te verkry nie. Aflaai van privaat E-pos van eksterne posrekeninge (bv. Hotmail, Yahoo, MSN, ens.) is verbode.

### VIRUSSKANDERING VAN E-POS:

Alle inkomende en uitgaande elektroniese pos moet voor versending vir virusse geskandeer word. Die skandering moet aanhangsels, hetsy gekompakteer ('zipped') of nie, insluit. Die uitsondering is geëinkripteerde e-pos. Spesifieke beleide wat geënkripteerde pos dek, kan in hierdie geval van toepassing wees.

## STANDAARD E-POSVRYWARING

Die vrywaring ('disclaimer') verskyn as die voetskrif onder-aan die e-pos en word normaalweg as 'n verstekteks geskep wat outomaties toegepas word wanneer 'n nuwe e-pos geskep word. Dit word normaalweg as 'n skryfbehoefte-element in e-poskliënte se konfigurasie geskep. Dit is die IT-departement se verantwoordelikheid om toe te sien dat die vrywaring outomaties op gebruikers se rekenaar of e-pos kliënt gekonfigureer word.

Die doel van die vrywaring is om die Munisipaliteit te beskerm teen litigasie as gevolg van die toevallige openbaarmaking van inligting aan 'n onbedoelde derde party, teen skade aan 'n derde party se rekenaarstelsel as gevolg van 'n rekenaarvirus of enige ander skadelike program wat in 'n e-posboodskap of aanhangsel by 'n e-posboodskap versteek of ingebed is.

Die e-posvoetreël, moet benewens die vrywaring, die naam van die organisasie waarvandaan die e-pos versend word en die e-posversender se naam en kontakbesonderhede bevat. Dit word vereis sodat enige indiwidu wat 'n e-pos onbedoeld ontvang, die opsteller in kennis kan stel en die e-pos kan vernietig sonder om enige afskrifte van die e-pos te behou.

# BYLAE A

## KAAP AGULHAS MUNISIPALITEIT E-POS VRYWARING ("DISCLAIMER")

E-Mail sent by the Cape Agulhas Municipality is to be treated as confidential, and the information in it may not be used or disclosed except for the purpose for which it has been sent. If you have reason to believe that you are not the intended recipient of this communication, please contact the sender immediately. Please then delete the message and do not disclose its contents to any person. Neither the sender nor Cape Agulhas Municipality accepts any liability whatsoever as a result of the further dissemination of this message. Whilst all reasonable steps are taken to avoid corruption of data or information, we do not accept any liability should such corruption occur. No employee or agent is authorized to conclude any binding agreement on behalf of the Cape Agulhas Municipality with another party by E-Mail without express written confirmation by the Cape Agulhas Municipality.

E-pos wat deur Kaap Agulhas Munisipaliteit versend is, moet as vertroulik beskou word en die inligting daarin mag nie gebruik word of openbaar gemaak word behalwe die doel waarvoor dit gestuur is nie. Indien u rede het om te glo dat u nie die bedoelde ontvanger van hierdie kommunikasie is nie, skakel asseblief onmiddellik die afsender. Skrap dan asseblief die boodskap en moet nie die inhoud aan enige persoon openbaar maak nie. Nog die afsender, nog Kaap Agulhas Munisipaliteit, aanvaar enige aanspreeklikheid as gevolg van die verdere verspreiding van hierdie boodskap. Hoewel alle redelike stappe gedoen word om korrupsie van inligting te verhoed, aanvaar ons geen aanspreeklikheid indien sodanige korrupsie sou plaasvind nie. Geen werknemer of agent is gemagtig om enige bindende ooreenkoms namens die Kaap Agulhas Munisipaliteit met 'n ander party per e-pos aan te gaan sonder uitdruklike skriftelike bevestiging deur die Kaap Agulhas Munisipaliteit nie.

# BYLAE B

## AANVAARDING VAN BELEIDSVOORWAARDES

Ek bevestig hiermee dat ek die terme en voorwaardes in hierdie beleid gelees het. Indien ek nie hierdie Beleid nakom nie, erken ek dat ek aan dissiplinêre optrede soos hierin vervat, onderhewig sal wees.

…… **WERKNEMERNOMMER**

…… **VOLLE NAAM EN VAN**

…… **DEPARTEMENT**

…… **AFDELING**

…… **HANDTEKENING**

…… **HANDTEKENING VAN GETUIE**

Geteken te ……op hierdie ……dag van……20…….

---

# BYLAE C

# NAKOMINGSOOREENKOMS

## OOREENKOMS OM INLIGTINGSEKERHEIDSBELEIDE NA TE KOM

Gebruiker se Naam in Duidelike Drukskrif:
_____

E-posadres: _____ Werknemerno.: _____

Departement: Posbenaming: _____
_____

Gebruiker se Telefoonnommer (Uitbreiding ingesluit): _____

Fisiese adres van Gebruiker se Kantoor:
_____

Gebruiker se IP Adres: _____

_____

Ek verstaan dat ek nie gemagtig is om hierdie inligting vir my eie doeleindes te gebruik nie en dat ek ook nie hierdie inligting aan ’n derde party mag voorsien sonder die uitdruklike skriftelike toestemming van die Munisipale Bestuurder wat die aangewese inligtingseienaar is. Ek onderneem om alle inligting waartoe ek toegang gehad het uit hoofde van my posisie by die Munisipaliteit met beëindiging van my diens of kontrak met die Munisipaliteit aan die Munisipaliteit terug te besorg.

Ek het toegang tot afskrifte van die Munisipaliteit se IT-beleide, ek het die inhoud van die Beleid gelees en verstaan dit, en ek verstaan hoe dit my posisie by die Munisipaliteit raak. As ’n voorwaarde van voortgesette diens by die Munisipaliteit, onderneem ek om hierdie inligtingsekerheidsbeleide na te kom. Ek verstaan dat nie-nakoming gronde vir dissiplinêre optrede bied tot en met stelselvoorregterugtrekking, ontslag uit die Munisipaliteit en moontlik kriminele en/of siviele strafbepalings.

Ek onderneem om ’n wagwoord te kies wat moeilik is om te raai, soos voorgeskryf in die Munisipaliteit se Inligtingsekerheidswagwoordstandaardedokument soos in hierdie Beleid bespreek. Ek onderneem om nie hierdie wagwoord met enige ander persoon te deel nie en ek onderneem om nie hierdie wagwoord neer te skryf nie tensy dit op ’n onherkenbare manier verander is.

Ek sal toesien dat net wettige en gelisensieerde programmatuur op die rekenaar geïnstalleer word en aanvaar dat die Munisipaliteit nie aanspreeklik gehou kan word vir enige oortredings as gevolg van my optrede nie.

Ek onderneem ook om alle oortredings of vermeende oortredings van inligtingsekerheidsbeleide spoedig aan die Bestuurder van IT en my direkte Bestuurder te rapporteer.

Ek onderneem dat die terme en voorwaardes van hierdie Nakomingsooreenkoms beide redelik en nodig is vir die beskerming van die Munisipaliteit se interne inligting, of inligting wat deur derde partye aan die Munisipaliteit toevertrou is.

Handtekening

Gebruiker:_____

Datum:_____

Gebruiker se Bestuurder:

_____

Datum:_____

_____