

BERGRIVIER MUNISIPALITEIT



IT-BELEID (INTERNET EN ePOS)

GOEDGEKEUR / APPROVED : RB 887

DATUM / DATE : 28 SEPTEMBER 2010

INHOUDSOPGAW

1. Doel
2. Definisies
3. IT Komitee (In proses en moet nog gekoördineer word)
 - 3.1 Standaard sagteware
 - 3.2 Standaard hardeware vereistes
 - 3.3 Bufferstoor
 - 3.4 Biblioteek
 - 3.5 Verskaffers
 - 3.6 Uitgediende toerusting
 - 3.7 Handeling met uitgediende rekenaartoerusting
 - 3.8 Sagteware deur IT Tegnici bestuur
4. Behoeftebepalings en Begrotings
5. Rekenaaropleiding
6. Rugsteun
7. Virusbeheer
8. Roofprogramme
9. Sekuriteit
10. Onderhoud
11. Foutrapportering
12. Algemeen
13. Liassering van Elektroniese Data

Bylae A IT Komitee se Verantwoordelikhede (Helpstasies)

Bylae B Goeie Praktykskode ("Code of Conduct")

Bylae C Magtigingsvorm vir die Verwydering van Rekenaartoerusting vanaf Raadspersele

Bylae D Internet en E-posbeleid
Annexure 1: Internet and eMail Declaration

Bylae E Disaster Recovery Plan

1. DOEL

Die doel van hierdie beleidsdokument is om standaardisasie en eenvormigheid in die raad ten opsigte van rekenarisering te bewerkstellig deur die riglyne van hierdie beleidsdokument te handhaaf. Dit is belangrik dat alle rekenaarverwante aankope en digitale kommunikasie verwante uitbreidings deur die IT-komitee geëvalueer en goedgekeur moet word.

2. DEFINISIES

CADDIE - rekenaarondersteunde teken en ontwerp

Deelware (“Shareware”) - sagteware waarop kopiereg bestaan waarvan kopiëring van sulke sagteware wettig is solank aan die voorgeskrewe gebruiksvereistes voldoen word.

ePos(eMail) - versending van data/dokumente in 'n digitale formaat d.m.v. rekenaartoerusting en kommunikasielyne (faksmasjiene uitgesluit)

GIS - geografiese informasiestelsel in digitale formaat

Internet - 'n digitale verbinding van internasionale **webtuistes** d.m.v. rekenaartoerusting en kommunikasielyne

Intranet - 'n digitale verbinding van die raad se interne **webtuistes** d.m.v. rekenaartoerusting en kommunikasielyne

IT-Komitee - 'n komitee saamgestel deur die raad wat, na oorweging van voorstelle voorleggings en aanbevelings t.o.v. rekenaarverwante aangeleenthede, aan die raad maak (Besig met samestelling)

Roofprogramme - enige sagteware waarop kopiereg bestaan en waarvan die ongemagtigde kopiëring daarvan verbied word en waar iemand ongelisensiëerd in besit is van so 'n kopie op rekenaar of diskette.

Rugsteun - die terugskryf van data na 'n tweede, vaste of vervoerbare medium wat op 'n alternatiewe plek gestoor word

Sluikpos (“Spoofing”) - Die tegniek om ongemagtigde inligting op 'n rekenaar te probeer verkry deur boodskappe te stuur na 'n rekenaar met 'n IP-adres wat blyk dat dit van 'n bekende persoon/rekenaar afkomstig is.

Telemetrie - die beheer/meet van toerusting deur middel van digitale kommunikasie oor lang afstande.

USB - “Universal Serial Bus” word gebruik om goedgekeurde toerusting aan 'n rekenaar te koppel sonder om af te skakel of sagteware te laai en onmiddellike gebruik daarvan te bewerkstellig.

Virus - 'n Self-uitvoerbare program wat so geskryf is dat dit data of programmatuur totaal of gedeeltelik kan uitwis/verander en daardeur skade aan die gebruiker berokken.

Vryware (“Freeware”) - sagteware wat gratis aan gebruikers beskikbaar gestel word vir evaluering en beperkte gebruik.

Webtuiste - 'n digitale (elektroniese) bron van data/inligting op rekenaar waartoe ander persone toegang verkry d.m.v. rekenaartoerusting en kommunikasielyne (koppeling met die Internet).

Wurm - 'n Wurm is soortgelyk aan 'n virus, aangesien dit 'n rekenaarprogram is wat self repliseer (vermenigvuldig) en kan funksionaliteit bevat wat inmeng met die normale gebruik van 'n rekenaar of program. Anders as virusse, is wurms eie entiteite; hulle heg nie aan ander leers of programme nie en kan self versprei oor 'n netwerk van een rekenaar na 'n ander deur gebruik te maak van die outomatiese "stuur en ontvang" funksies van rekenaars.

3. IT-KOMITEE

In proses en samestelling sal so gou moontlik geskied.

3.1 STANDAARD SAGTEWARE/PROGRAMMATUUR

Standaard sagteware verseker dat alle rekenaartoerusting met mekaar kan kommunikeer en dat data maklik tussen direkteur/departemente en gebruikers uitgeruil kan word. Dit vorm ook die basis van eenvormigheid vir alle standaard dokumente wat die raad mag produseer. Die lys van standaard produkte kan na gelang van omstandighede deur die IT-komitee aangepas word.

3.2 STANDAARD HARDEWARE VEREISTES

Standaard hardeware verseker dat alle rekenaars die vermoë sal hê om alle sagteware in gebruik in die raad te kan bedryf. Die hardeware moet ook die vermoë hê om opgradeerbaar te wees. Die lys van standaard produkte kan na gelang van omstandighede deur die IT-komitee aangepas word.

3.3 BUFFERSTOOR

Bufferstore sal departementeel deur die IT-komitee lede bedryf word vir noodsaaklike rekenaartoerusting wat onmiddellik vervang moet word.

3.4 BIBLIOTEEK

'n Biblioteekstelsel sal per verantwoordelike area deur die IT-komitee bedryf word waar alle noodsaaklike sagtewarehandleidings (indien beskikbaar in hardekopie formaat) gestoor sal word.

3.5 VERSKAFFERS EN ONDERSTEUNINGSDIENSTE

'n Lys van verskaffers/ondersteuningsdienste sal bygehou word deur die IT-komitee vir voorkeurdienste en lewering aan die raad. Daar sal gepoog word om so ver moontlik plaaslik te ondersteun. Die lys kan na gelang van omstandighede deur die IT-komitee aangepas word.

3.6 UITGEDIENDE TOERUSTING

Daar moet verhoed word dat die raad die Wet op Kopiereg oortree met die verkoop van uitgediende rekenaartoerusting. Geen hardeskywe of datadiskette mag per openbare veiling of aan lede van die publiek verkoop word nie, aangesien metodes (sagteware) bestaan om data van sulke skywe en diskette te herwin.

3.6.1 Uitgediende toerusting moet ooreenkomstig die Raad se Batebeleid binne die raad herontplooi word in direkte/departemente waar die behoefte vir minimale of afgeskaalde gebruik ontstaan.

3.6.2 Uitgediende sagteware (oorspronklike diskette en CD-ROMs) kan met Raadsgoedkeuring aan die agtergeblewe gemeenskappe se skole geskenk word, slegs as sodanige kopiereg/lisensie van die betrokke sagteware die oordrag van eienaarskap sou toelaat.

3.6.3 Diskette waarvan die oordrag van eienaarskap deur die kopiereg/lisensie verbied word, kan skoongemaak word en vir interne gebruik as skoon datadiskette aangewend word.

3.6.4 Geen hardeskywe of datadiskette mag per openbare veiling verkoop of aan lede van die publiek oorhandig word nie. Daar moet verseker word dat datadiskette wat vir werksdoeleindes aan die publiek of ander maatskappye verskaf word, nie sensitiewe data bevat nie. Verkieslik moet skoon diskette gebruik word.

3.6.5 Uitgediende diskette wat nie hergebruik kan word nie, moet deur die IT-komitee vernietig word of in die liasseerstelsel geplaas word.

3.6.6 Daar moet met die vervreemding van rekenaartoerusting volgens die raad se Batebeleid gehandel word.

3.7 HANDELING MET UITGEDIENDE REKENAARTOERUSTING

Hierdie maatreëls moet nagekom word wanneer met uitgediende rekenaartoerusting gehandel word:

3.7.1 Funksionele rekenaars, wat net verouder is en vir minder intensiewe take aangewend kan word in ander direkte/departemente of afdelings, kan oorgeplaas word deur die vorm "Handeling met Bates" te voltooi en by die Batebeheerbeampte in te handig, waardeur die nuwe ligging van die toerusting dan op lêer geplaas sal word. Die nuwe departement is verantwoordelik vir die dag-tot-dag onderhoudskostes van die bate. Prioriteit moet gegee word aan die ontplooiing binne eie departement.

- 3.7.2 Rekenaartoerusting wat nie herontplooï/hergebruik kan word nie, moet van noodsaaklike onderdele gestroop word en die res by die Magasyn indien met die vorm "Handeling met Bates" waarna 'n kwitansie deur die Magasyn uitgereik sal word en vanwaar dit per openbare veiling verkoop sal word.
- 3.7.3 Gestroopte onderdele moet in die Bufferstore geberg word en 'n volledige bygewerkte inventarislys van alle onderdele moet aan die IT Komitee voorsien word met elke vergadering.
- 3.7.4 Uitgediende bruikbare onderdele, behalwe bewaarmediums, moet by die Magasyn ingedien word vanwaar dit per openbare veiling verkoop sal word.
- 3.7.5 Uitgediende onbruikbare onderdele, behalwe bewaarmediums, kan mee weggedoen word.

3.8 SAGTEWARE WAT DIE IT KOMITEE BESTUUR

- 3.8.1 Microsoft Server Client Access Licensing
- 3.8.2 Microsoft Exchange Server Client Access Licensing
- 3.8.3 Trend Micro Antivirus Server Engine and Patterns
- 3.8.4 Proxy sagteware

4. BEHOEFTEBEPALINGS EN BEGROTINGS

Die IT-Komitee

- 4.1 Evalueer behoeftebepalings wat departementeel afgehandel en voorgelê is;
- 4.2 Evalueer globale behoeftebepalings met inagneming van die uitbreiding van gesentraliseerde stelsels en die skryf van verslae aan die raad;
- 4.3 Evalueer behoeftes en moontlike wysigings en beveel begrotingsbedrae aan vir die direktorate/departemente voordat begroot kan word;
- 4.4 Adviseer direktorate/departemente oor die bedrae wat uit die begroting uitgesluit kan word;
- 4.5 Is verantwoordelik vir die opstel van tenderdokumente, die vra van kwotasies en die aankoop van rekenaartoerusting, met inbegrip van die uitreik van rekwisisies; en

4.6 Is verantwoordelik vir verslae aan die raad t.o.v. tenders en verwante aangeleenthede; asook vir die toekenning en plasing van rekenaartoerusting wat per tender/kwotasie aangekoop word.

5. REKENAAR OPLEIDING

Rekenaarverwante opleiding sal deur Menslike Hulpbrondienste in samewerking met die IT-komitee bestuur word. Direkorate/departemente is egter welkom om spesifieke opleidingsbehoefte aan die IT-komitee skriftelik deur te gee.

6. RUGSTEUN

Alle data moet daaglik gerugsteun word. Waar die gerief bestaan moet outomatiese rugsteunfasiliteite gebruik word. **Rugsteun bly die verantwoordelikheid van die gebruiker van sodanige data.**

7. VIRUSBEHEER

7.1 Virusbeheer van alle rekenaars moet op 'n outomatiese basis geskied.

7.2 Voordat enige diskette in die rekenaar gebruik word, moet dit eers vir virusse getoets word.

7.3 Virusdefinisies moet minimum weekliks bygewerk word.

7.4 Virusdefinisies ouer as 8 dae word nie as 'n geldige virusprogram geag nie.

7.5 Elke rekenaargebruiker is self verantwoordelik vir die beheer en voorkoming van virusse op sy/haar toerusting.

8. ROOFPROGRAMME

8.1 Geen roofprogramme word toegelaat nie.

8.2 Roofprogramme alreeds in gebruik moet sonder versuim gewettig of van die stelsels verwyder word.

8.3 Sogenaamde "shareware" en "freeware" is nie onwettig op rekenaars nie, maar die blootstelling aan ander onbekende rekenaars maak dit 'n risiko in die verspreiding van virusse en word dus nie aanbeveel nie. Waar dit 'n besparing vir die raad regverdig, kan dit toegelaat word na oorlegpleging met die IT-komitee. Daar moet egter aan die gebruiksvoorwaardes voldoen word.

8.4 Personeel wat onwettige roofprogramme op die raad se rekenaars laai, toelaat om te laai of gebruik, kan ingevolge die dissiplinêre prosedure aangekla word.

9. SEKURITEIT

- 9.1 Maatreëls bestaan waarvolgens rekenaars deur die gebruik van wagwoorde beskerm kan word en behoort toegepas te word waar sensitiewe en belangrike inligting of data na ander partye kan uitlek of deur ander partye uitgewis kan word.
- 9.2 Gebruikers moet rekenaars afskakel of beveilig deur wagwoorde wanneer:
 - 9.2.1 die gebruiker vir langer as 3 minute van die kantoor afwesig gaan wees
 - 9.2.2 lede van die publiek alleen by 'n gebruiker se rekenaar agtergelaat word
 - 9.2.3 ander ongemagtigde personeel alleen by die rekenaar agtergelaat word
 - 9.2.4 die gebruiker met ete of huis toe gaan
- 9.3 Gebruikers moet rekenaarskerms afskakel of beveilig deur wagwoorde indien met sensitiewe inligting gewerk word en die inligting nadelig/negatief aangewend kan word deur 'n lid van die publiek of ander ongemagtigde personeel wat die gebruiker besoek en dit op daardie manier kan besigtig.
- 9.4 Voordat rekenaars van die raad se persele verwyder word, moet 'n magtigingsbrief (**BYLAE C**) voltooi word wat ten alle tye in die werknemer wat die toerusting verwyder se besit sal wees.

10. ONDERHOUD

Die volgende inligting moet te alle tye by elke rekenaar van die raad teenwoordig wees:

- 10.1 Logstaat van instandhouding
- 10.2 Inventaris van harde- en sagteware

11. FOUTRAPPORTERING

- 11.1 Alle foute moet direk aan die IT-tegnikus gerapporteer word wat die nodige stappe sal neem om die herstel te bewerkstellig - geen ongemagtigde persone mag aan rekenaartoerusting werk nie.
- 11.2 Enige abnormale verskynsels moet dadelik aan die verantwoordelike Komiteelid gerapporteer word - alle verwerkings moet dadelik gestaak word.

11.3 Enigiemand wat bewus word van die ongemagtigde gebruik van rekenaars moet dit onverwyld rapporteer aan lede van die IT-komitee.

12. ALGEMEEN

12.1 ROOK BY REKENAARTOERUSTING WORD VERBOD.

12.2 Geen rekenaaraktiwiteit wat nie besigheidsverwant is nie, mag op rekenaars ge-aktiveer word tydens werksure nie.

12.3 Geen ongemagtigde persoon mag toerusting oopmaak of bedryf nie.

12.4 Toerusting mag nie ontkoppel word terwyl dit aangeskakel is nie, uitgesluit USB- gekoppelde toerusting.

12.5 Die persoon aan wie 'n rekenaar toevertrou word is verantwoordelik vir die goeie sorg daarvan.

12.6 Gebruikers moet hulself vergewis van al die voordele wat die sagteware kan bied deur die bestudering van handleidings.

12.7 Rekenaars moet met een of ander vorm van goedgekeurde stuwingsbeskerming (weerligafleiers) toegerus wees.

12.8 Gebruikers moet vloeistowwe en kos weg van rekenaars hou om te verhoed dat rekenaartoerusting beskadig word. Vogtige lug, asook rook, mag nie toegelaat word om oor die rekenaartoerusting te waai nie.

12.9 Rekenaars mag net rondgeskuif word as 'n IT-technikus teenwoordig is.

12.10 Die waaiers in die verwerkerkas se lugvloei mag nie versper word nie.

12.11 Die hoogste moontlike posisie vir die rekenaar word aanbeveel om stofaanpakking en skade te voorkom.

12.12 Voordat 'n nuwe gebruiker van die rekenaartoerusting gebruik maak, moet hy in besit gestel word van hierdie rekenaarbeleidsdokument en dit onderteken.

12.13 Geen verwerker en geheue intensiewe skermbewaarder sal op rekenaars toegelaat word nie.

12.14 Geen sterk oplosmiddels mag in kamers/kantore waar duur elektroniese rekenaartoerusting bedryf word, gebruik word nie.

13. LIASSERING VAN ELEKTRONIESE DATA

- 13.1 Alle elektronies gegenereerde data/dokumente van die raad wat publieke belang het of belangrike inligting vervat, moet volgens die Nasionale Argiefwet in die Liasseerstelsel in goedgekeurde media opgeneem word.
- 13.2 Goedgekeurde media wat aanvaar word is papier, magnetiese band, kompakskyf (CD) en DVD.
- 13.3 Wanneer na nuwe programme oorgeskakel word, moet die ou data eers omgeskakel word na die nuwe stelsel alvorens dit vir bewaring geliasseer word. Waar ou data nie omgeskakel kan word nie, moet die ou hardeware (stelsel) behou word. Die raad moet dus verseker dat data sinvol gelees kan word jare nadat dit gegenereer is.

IT PERSONEEL VERANTWOORDELIKHEIDSLYS

Die onderstaande personeel met gelysde verantwoordelikhede kan gekontak word in verband met enige tersaaklike probleme:

Lys sal moet op gestel word en spesifieke personeelede sal moet aangestel word na oorleg en konsultasie.

Fisiese WAN Koppeling

Shane Lesch

Hardeware of Sagteware wat nie gelys is nie, word nie noodwendig nie-amptelik ondersteun nie en navrae in die verband kan aan die IT- Tegnikus gerig word.

Goeie Praktykskode vir Rekenaargebruikers

Elke personeelid wat rekenaartoerusting ontvang het vir gebruik in die uitvoering van sy/haar daaglikse pligte sal verantwoordelik gehou word vir sodanige toerusting solank as wat hy/sy in diens van hierdie Raad is. Enigiets wat nie uitdruklik deur hierdie dokument en die rekenaarbeleidsdokumente toegelaat word nie, word streng verbied, met die uitsondering van 'n voltooide magtigingsvorm van die verantwoordelike IT-komiteelid, asook die Hoof van die betrokke Departement. Die gebruiker onderneem om die voorwaardes van hierdie beleid na te kom. Die rekenaartoerusting sal hoofsaaklik vir raadsgebruik aangewend word en enige nie-winsmakende privaatgebruik is slegs toelaatbaar met die toestemming/magtiging van die betrokke departementshoof.

1. Hardeware

- (i) Geen toerusting mag van die Raad se perseel verwyder word sonder die nodige voltooide magtigingsvorm soos gestipuleer deur die Raad se IT-beleid nie.
- (ii) Geen toerusting mag oopgemaak/uitmekaar gehaal word nie, behalwe deur die verantwoordelike IT-komitee personeel. As probleme ontstaan, moet dit so gou as moontlik aan die verantwoordelike IT-komiteelid gerapporteer word.
- (iii) Dit is die gebruiker se verantwoordelikheid om seker te maak dat die toerusting in goeie werkende toestand gehou word, vry van stof, rook en enige ander degraderende stowwe. Periodieke beplande onderhoud sal gedoen word deur die IT Komitee of 'n verantwoordelike persoon wat aangewys sal word.
- (iv) Die toepaslike skoonmaakmiddels sal beskikbaar gestel word op versoek. Dit is die enigste middels wat toegelaat sal word om die toerusting mee skoon te maak.

2. Sagteware

- (i) Dit is elke gebruiker se verantwoordelikheid om seker te maak dat geen onwettige sagteware op die rekenaar gelaai is nie. Alle onwettige sagteware moet so gou as moontlik aan die IT-komitee gerapporteer word om dit te verwyder of te wettig.
- (ii) Rekenaargebruikers sal verantwoordelik gehou word vir alle sagteware op hulle rekenaars asook enige onkoste wat veroorsaak word deur onwettige sagteware of die gebruik daarvan.
- (iii) Oorspronklike lisensies en diskette van sagteware wat wettig gelaai is, moet deur die IT-tegnikus bewaar word.

- (iv) Die Raad, gedelegeer aan die IT-technikus, sal die lisensies vir die gesentraliseerde stelselsagteware voorsien en bewaar.
- (v) Enige rekenaartoerusting mag ter enige tyd deur die IT-komitee geoudit word om te verseker dat alle toerusting wettig en vir raadsgebruik aangewend word. Die raad se IT tegnici het die nodige magtiging om 'n oudit te doen in opdrag van die betrokke departementshoof en / of die Munisipale Bestuurder.
- (vi) Alhoewel algemene oorhoofse beskerming vir die raad se netwerke teen virusse aangeskaf sal word, is dit nog steeds die gebruiker se verantwoordelikheid om seker te maak dat geen besmette data, speletjies of onwettige sagteware op die rekenaar gelaai word nie, asook om die periodieke skandering van die hardeskyf te doen.
- (vii) Die gebruiker van die rekenaar sal aanspreeklik gehou word vir enige onweloweglike sagteware, agtergrondskermbeelde, skermbewaarders, ens. Die verspreiding van onwettige of onaanvaarbare data boodskappe word nie toegelaat nie.
- (viii) Die gebruiker van die rekenaar sal aanspreeklik gehou word om toe te sien dat die rekenaar voltyds by die netwerkbedieners ingeskakel is, om te verseker dat die antivirus program suksesvol kan funksioneer.
- (xi) Gebruikers wat met ePos toegerus is moet die ePos program deurentyd geaktiveer hou. Slegs waar die ePos program die werking van die rekenaar of ander sagteware erg benadeel, mag dit tydelik gedeaktiveer word.

3. **Privaat Rekenaartoerusting**

- (i) 'n Volledig voltooide magtigingsvorm moet verkry word van die betrokke Hoof van die Departement en die IT-komiteelid vir enige rekenaartoerusting (insluitend alle hardeware en sagteware) wat die Raad se perseel verlaat of binnekom.
- (ii) Die gebruiker verklaar dat enige privaat toerusting wat die stelsels nadelig beïnvloed en sonder 'n magtigingsvorm gebruik word, gekonfiskeer mag word deur die IT-komitee.
- (iii) Privaattoerusting moet voor gebruik na 'n netwerkadministrateur vir virus en aanpasbaarheidstoetse geneem word voordat dit op die raad se netwerkstelsels gebruik/gekoppel mag word.
- (iv) Geen data/sagteware mag oorgelaai word van privaattoerusting na enige van die Raad se toerusting voordat 'n virus skandering gedoen is nie.

- (v) Die Raad aanvaar geen verantwoordelikheid of aanspreeklikheid vir enige verlies, beskadiging of onkoste voorspruitend uit die gebruik van enige privaattoerusting nie.

4. **Eksterne Verbindings**

- (i) Gebruikers se toegang tot die ePos sal beperk wees tot spesifieke goedgekeurde gebruikers.
- (ii) Webtuistes vanwaar inkomende ePos toegelaat sal word, sal deur die IT-komitee vir sekuriteitsdoeleindes beperk word.
- (iii) Die raad se interne ePos adreslys mag nie aan enige partye buite die Raad beskikbaar gemaak word sonder die toestemming van die Munisipale Bestuurder nie.
- (iv) Gebruikers van die Internet sal verantwoordelik gehou word vir alle ongewenste data wat afgelaai is van webtuistes en enige gevolge wat dit mag hê.

MUNISIPALITEIT BERGRIVIER

MAGTIGINGSVORM VIR DIE VERWYDERING/INBRING VAN TOERUSTING VANAF/NA RAADSPERSELE EN KOPPELING VAN PRIVAAT TOERUSTING AAN DIE REKENAARNETWERK

Hierdie volledig voltooide vorm moet alle rekenaartoeusting vergesel wat van/na die raad se persele verwyder/gebring word, ongeag of dit vir die doel van tuisgebruik, kursusse of herstelwerk is en sluit rugsteuningsmedia in; OF die koppeling van enige privaat rekenaartoeusting aan die raad se rekenaarnetwerk.

Aansoeker: _____ **Datum:** ____/____/____

Doel _____ **van** _____ **Verwydering** _____ **/** _____ **Koppeling:** _____

Batenommers: _____; _____;

Beskrywing van Bate/Toerusting: _____

As aansoeker vir die verwydering van rekenaartoeusting vanaf die raadsperseel verklaar ek dat ek nie sal toelaat dat:

- (i) Die raad se rekenaartoeusting vir privaat doeleindes aangewend sal word nie;
- (ii) Inligting op die rekenaar aan ongemagtigde persone of instansies deurgegee sal word nie;
- (iii) Inligting op die rekenaartoeusting ongemagtig aangewend sal word nie;
- (iv) Onderdele uitgeruil, verwyder of mee gepeuter sal word nie;
- (v) Rekenaartoeusting opsetlik gedegradeer sal word nie;
- (vi) Rekenaartoeusting in ongemagtigde derde partye se hande beland nie;
- (vii) Ongewenste materiaal, virusse of onwettige sagteware op die rekenaar gelaai sal word nie.

Omvang van Herstelwerk/Opgradering (lys komponente in dien moontlik):

Voorwaardes (indien enige): _____

Aansoeker

Departementshoof

Verteenwoordiger: IT-komitee

INTERNET AND eMAIL POLICY

1. Policy overview

This Internet and email usage policy is designed to help you understand Council's expectations for the effective use of resources in the particular conditions of the Internet environment. The Internet and email facilities for Bergrivier Municipality, hereafter referred to as Council, is a business tool, provided to you at significant cost to:

1. Use your Internet and email access for business related and/or educational purposes;
2. Conduct yourself honestly within existing Council Policies;
3. Respect Copyrights, Software licensing rules and Property rights;
 - (i) Unnecessary or unauthorized Internet and email usage causes network and server congestion. Unlawful Internet and email usage may also garner negative publicity for Council and exposes the council to significant legal liabilities.
 - (ii) Users must take special care to maintain the clarity, consistency and integrity of Council's corporate image and posture.
 - (iii) Internet and email also opens the door to some significant risks to our data and systems if we do not follow appropriate security discipline.
 - (iv) All employees granted Internet and email access with Council facilities will be provided with a written copy of this policy and must sign the attached declaration; opting not to sign will be seen as not being in need of these facilities, where after all access rights will be terminated.

2. Management and Administration

- (i) Council has software and systems in place that monitor and record all Internet and email usage. Although the Internet and email usage won't be monitored by a member of the IT Committee on a daily basis, no employee should have expectations of privacy as to his or her Internet and email usage.
- (ii) Management reserves the right to inspect any and all files stored in public and private areas of our network in order to assure compliance with this policy.

- (iii) Internet facilities and computing resources must not be used to knowingly violate the laws and regulations of South Africa or the applicable laws and regulations of international bodies or governments.
- (iv) No employee may use Council facilities to knowingly download or to distribute pirated software or data, or to deliberately propagate any virus, worm, Trojan horse, or trapdoor program code or to knowingly disable or overload any computer system or network, or to circumvent any systems intended to protect the privacy or security of another user or institution.
- (v) No employee shall distribute the email address list of Council to a third party for marketing and/or advertising purposes, nor may it be used for chain mail or offensive marketing.
- (vi) No employee, other than the Municipal Manager or officials who are duly authorized by him, may speak, or write and/or sign documents, on behalf of Council. Employees may participate in newsgroups or chat forums in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves, unless otherwise authorised to speak on behalf of Council.
- (vii) Employees are reminded that chat and newsgroups are public forums where it is inappropriate to reveal confidential Council information, customer data, trade secrets or any other material covered by existing Council secrecy policies and procedures.
- (viii) The Council will limit Internet and email access to those employees who demonstrate a legitimate business or educational need.
- (ix) It is a violation of Council policy to store, view and print or redistribute any sensitive document or graphic file that is not directly related to the user's function or Council's business activities.
- (x) Private email messages may be received and sent by users, but should be kept to an absolute minimum and should not include massive data, graphics or media files.
- (xi) Misuse of the Internet and email facilities may lead to permanent disconnection of a user by order of management and may result in disciplinary steps against such an employee.
- (xii) Employees may use their Internet and email facilities for non-business research or browsing during mealtimes, tea-breaks or outside of working hours, unless otherwise authorized, provided that all other Council policies are adhered to.

- (xiii) Employees with Internet and email access may only download software, with written authorization of the IT Committee, for direct business purposes and must arrange to have such software properly licensed and registered. Downloaded software may only be used under the terms of the relevant license agreements.
- (xiv) Employees with Internet and email access may not use Council Internet facilities to download entertainment software or games, nor to play games against opponents over the Internet or network.
- (xv) Employees with Internet and email access may not use Council Internet facilities to download videos, presentations or audio (music), unless there is an explicit business related use for the material. Employees with Internet access may not listen to radio or television channels over the Internet.
- (xvi) Employees with Internet and email access may not upload or email any software licensed to Council or data owned or licensed by Council, without explicit written authorization from the responsible member of the IT Committee for the software and data integrity of Council for that department.
- (xvii) Employees with Internet and/or email access may not distribute data that may be termed offensive, nor may they visit websites which could be construed as being offensive.

3. Technical

- (i) User ID's and passwords help maintain individual accountability for Internet and email resource usage. Any employee who obtains a password or ID for an Internet and email resource must keep that password confidential and private.
- (ii) Employees should schedule communication-intensive operations such as large file transfers, video downloads, mass mailings and the likes for off-peak times. Large files must be compressed before sending or receiving.
- (iii) Any file that is downloaded must be scanned for viruses, worms, Trojan Horses and trapdoor computer code or any other malicious content before it is opened/executed on a computer or in memory.
- (iv) Video and audio downloading should be avoided.

4. Security

- (i) The IT Committee has installed a firewall, screening programs and other security systems to assure the safety and security of Council networks. Any employee who attempts to disable, defeat or circumvent any security facility will be subject to a disciplinary hearing.
- (ii) File encryption must be used for secret and confidential documents sent and received over the Internet.

ANNEXURE 1

INTERNET AND EMAIL POLICY DECLARATION

I,

(Print name),

with personnel number: _____ have received a written copy of the Bergrivier Municipality's "INTERNET AND EMAIL USAGE POLICY". I have studied this aforementioned policy of Council and I fully understand the terms and conditions and agree to abide by it, whether signed by me or not.

I realise and acknowledge that the Bergrivier Municipality's security software, records for management's perusal, the Internet addresses (including date and time) of any site that I may visit.

I realise and acknowledge that Council's security software may also keep a record of all network activity of any kind, including inter alia email messages which I transmitted or received, as well as any files which have been transferred to or from my PC.

Should I wish not to sign this declaration, because I do not agree with its terms and conditions, I realise that I may be removed from the Internet and/or email access groups forthwith.

I understand that any violation of this policy could lead to disciplinary action.

IMPORTANT:

By the user making use of Council's Internet and/or email facilities he/she has de facto accepted Council's IT Policy.

Signature of User

Date

IT Committee Member

Date

BYLAE F

DISASTER RECOVERY PLAN

IN PROCESS (Estimated completion date 1 August 2012)...