

Richtlijn ICT-gebruik gemeente Heerlen

30 september 2004

**Gepubliceerd door Victor Abratanski,
Bureauhoofd ICT Services**

Status van het document

X	Ontwerp
	Publicatie

Versie

Datum	Versie	Beschrijving
2 mei 2004	V 1.01	Document in de maak.
7 september 2004	V 2.01	Document afgestemd met P&O
30 september 2004	V 2.02	Document goedgekeurd door directieraad

Gerelateerde producten:

- Regeling voor het gebruik van de telecommunicatiemiddelen door medewerkers van de Gemeente Heerlen
- Productencatalogus bureau ICT-Services
- Integriteitscode
- Nota "Verantwoord Internetgebruik door medewerkers van de gemeente Heerlen"

Inhoudsopgave

1. Algemeen gebruik

A. Reikwijdte van de handleiding	4
B. Doel	4
C. Verklaring	4
Aanvaardbaar gebruik	4
Verantwoordelijkheid i.v.m. wachtwoord	4
Inbreuk op beveiliging van informatie	5
Vertrouwelijkheid van informatie	5
Bescherming van auteursrechten en softwarelicenties	5
Gedragscode op incidenten i.v.m. beveiliging van informatie	5
Hoe te handelen bij virussen	5
Configuratiewijzigingen	5
Back-up van informatie	5
Inbelverbindingen	5
Gebruikersapparatuur zonder toezicht	6
Beveiliging van apparatuur	6
Recht op controle en onderzoek	6
D. Richtlijnen	
Verantwoordelijkheid i.v.m. wachtwoord	6

2. Softwarelicenties en -gebruik

A. Doelgroep	7
B. Doel	7
C. Verklaring	7
Alle software	7
Gespecialiseerde software	7
Verboden software	7
Kopieën van software met auteursrechten	7
Privé-gebruik van software van Gemeente Heerlen	7

3. Gedragsregels bij het gebruik van de internet- en e-mailvoorziening van gemeente Heerlen

A. Doelgroep	8
B. Doel	8
C. Verklaring	8
Viruspreventie en virusopsporing	8
Uitwisselen van informatie en transacties via Internet	8
Vertrouwelijkheid van informatie	8
Opslaan van e-mailcommunicatie	9

4. Overeenstemming

5. Aanspreekpunten

1. Algemeen gebruik

A. Reikwijdte van de handleiding

1. De regeling geldt voor iedere medewerker die gebruik maakt van de telecommunicatiemiddelen van de gemeente Heerlen en die aan te merken is als ambtenaar in de zin van artikel 1:1 lid 1 sub a van de CAR alsmede voor uitzendkrachten, detacheringkrachten, stagiaires en personen die anderszins (betaald of onbetaald) werkzaamheden verrichten voor de gemeente Heerlen.
2. Voor de toepassing van deze regeling wordt onder telecommunicatiemiddelen verstaan: telefoon, faxapparatuur, personal computer, overige communicatie- en informatietechnologische voorzieningen.

B. Doel

Het doel van deze handleiding is een richtlijn te bieden voor alle gebruikers van de informatie- en communicatietechnologische voorzieningen van Gemeente Heerlen. De ICT-voorzieningen omvat de desktops, pc's, notebooks, thin cliënts, PDA's, modems, netwerken, file servers, telefonievoorziening, faxtoestellen, etc. van Gemeente Heerlen.

C. Verklaring

Aanvaardbaar gebruik

- In het document "*Regeling voor het gebruik van de telecommunicatiemiddelen door medewerkers van de Gemeente Heerlen*" wordt dit item uitgebreid omschreven.

Verantwoordelijkheid i.v.m. wachtwoord

De gebruikers dienen er over geïnformeerd te zijn dat:

1. Men moet wachtwoorden opbouwen de criteria van een kwaliteitswachtwoord als onderstaand beschreven.
2. De gebruiker moet zijn wachtwoord geheimhouden en mag zijn LoginID en wachtwoord aan niemand vertellen.
3. De gebruiker mag zijn wachtwoord niet openlijk opschrijven.
4. Middelen voor toegangscontrole, zoals facilitaire sleutels, vaste wachtwoorden of andere toegangsmiddelen met anderen delen.
5. Als de systemen de gebruikers niet verplichten hun wachtwoord te wijzigen op vastgestelde tijdstippen, moeten de gebruikers ervoor zorgen dat ze hun wachtwoord om de 90 dagen wijzigen.
6. Het gebruik van PC boot-up wachtwoorden (BIOS wachtwoord bij opstarten) is zonder toestemming van bureau ICT-Services verboden. Het verdient de aanbeveling schermbeveiligingswachtwoorden (screensaver) te gebruiken om onwettige toegang te voorkomen wanneer men de toestellen aangesloten achterlaat zonder toezicht.
7. Men mag hetzelfde wachtwoord of ongeveer hetzelfde wachtwoord (teller ophogen) niet opnieuw gebruiken. Het opnieuw gebruiken van oude of aanverwante wachtwoorden is verboden binnen een periode van 12 maanden.
8. Als er enige aanwijzing is dat een wachtwoord bij anderen bekend is, of enige aanwijzing van een inbreuk op de beveiliging van de ICT-systemen van Gemeente Heerlen, gekend of vermoed, moet men het wachtwoord onmiddellijk veranderen. Eveneens dient direct melding te maken bij de Helpdesk van bureau ICT-Services.
9. Gebruikers die hun wachtwoord vergeten zijn, moeten dit melden aan de Helpdesk, die zal zorgen voor een nieuw tijdelijk wachtwoord. Tijdelijke wachtwoorden moet men wijzigen bij de eerste aanmelding.
10. Wachtwoorden mogen geen naam zijn of iets vergelijkbaars zoals de

- namen van kinderen, huisdieren, etc..
11. In geen geval mag het wachtwoord van een gebruiker hetzelfde zijn als zijn gebruikersnaam (LoginID).
 12. Gebruik geen wachtwoorden die men specifiek met u kan associëren, zoals geboortedatum, naam van familieleden en telefoonnummers.

Inbreuk op de beveiliging van informatie

Gebruikers mogen niet proberen testen uit te voeren voor het verkrijgen van toegang, nog enig onderzoek of enige activiteiten ondernemen die de toegangscontrole van de computervoorziening van Gemeente Heerlen compromitteren, tenzij men de beroepsnoodzaak daarvan kan aantonen en bureauhoofd ICT-Services vooraf de geschreven goedkeuring gegeven heeft voor dergelijke activiteiten en de voorwaarden waaronder die zullen plaatshebben.

Vertrouwelijkheid van informatie

In het document “Regeling voor het gebruik van de telecommunicatiemiddelen door medewerkers van de Gemeente Heerlen” wordt dit item uitgebreid omschreven.

Bescherming van auteursrechten en softwarelicenties

In het document “Regeling voor het gebruik van de telecommunicatiemiddelen door medewerkers van de Gemeente Heerlen” wordt dit item uitgebreid omschreven.

Gedragcode op incidenten betreffende de beveiliging

Echte of vermoede inbreuken op de informatiebeveiliging, zoals onrechtmatig gebruik van de wachtwoorden van andere gebruikers, onrechtmatig gebruik van de ICT-voorzieningen van Gemeente Heerlen, verspreiden van virussen, pogingen tot kraken van informatiebeveiliging, etc., moet men direct rapporteren aan de Helpdesk van Gemeente Heerlen.

Hoe te handelen bij virussen

- Gebruikers mogen niet zelf proberen zelf virussen te verwijderen. Als een gebruiker een virusinfectie ontdekt, moet het gebruik op de betreffende werkplek direct worden beëindigd en de werkplek direct uitschakelen. Vervolgens moet dit gerapporteerd worden aan de Helpdesk van bureau ICT-Services.
- Gebruikers mogen niet op eigen initiatief reageren op een virusalarm en moeten zich onthouden van het doorsturen van een virusalarm, behalve dan naar de Helpdesk van bureau ICT-Services. Al vaker is gebleken dat een virusalarm die verspreid werden via e-mail vals waren en alleen bedoeld zijn om het functioneren van het systeem te belemmeren.
- Gebruikers mogen e-mail berichten niet openen als ze vermoeden dat die een virus bevatten. Extra waakzaamheid is geboden bij afzenders welke men niet kent. Verdachte e-mail berichten moet men onmiddellijk melden bij de Helpdesk van bureau ICT-Services.

Configuratiewijzigingen

Gebruikers mogen niet proberen de configuratie van hun werkplek te wijzigen. De Helpdesk moet alle verzoeken om configuratiewijzigingen registreren en laten uitvoeren door medewerkers van bureau ICT-Services. Enkele voorbeelden zijn bijvoorbeeld Windows upgraden, instellingen in Windows wijzigen, nieuwe software installeren, modems installeren, randapparatuur koppelen.

Back-up van informatie

Alle bestanden moet men opslaan op het interne netwerk van Gemeente Heerlen dat speciaal voorzien is voor het opslaan van vertrouwelijke of kritische informatie, waar men ze kan beveiligen en er een back-up van kan maken conform het beleid van Gemeente Heerlen.

Inbelverbindingen

Gebruikers mogen zelf geen modemverbinding tot stand brengen aan de

computervoorzieningen van Gemeente Heerlen, tenzij men de beroepsnoodzaak daarvan kan aantonen en het bureauhoofd ICT-Services de verbinding vooraf schriftelijk goedgekeurd heeft. Het koppelen van computers niet beheerd door bureau ICT-Services aan het netwerk van Gemeente Heerlen wordt niet toegestaan.

Elke gebruiker met rechten om van buitenaf gebruik te kunnen maken van de ICT-voorzieningen van Gemeente Heerlen (inbelfaciliteit, telewerken, webmail) is verplicht zorg te dragen dat het netwerk van Gemeente Heerlen niet gebruikt wordt door personen die geen werknemer zijn van Gemeente Heerlen.

Gebruikersapparatuur zonder toezicht

Alle werkplekken die toegang hebben tot het netwerk van Gemeente Heerlen moet men beschermen met een door een wachtwoord geactiveerde schermbeveiliging wanneer men ze achterlaat zonder toezicht.

Beveiliging van apparatuur

- Computers, printers en andere niet-draagbare apparatuur die eigendom zijn van Gemeente Heerlen mag men niet verwijderen uit de kantoren tenzij ze vergezeld zijn van een goedgekeurd afvoerbewijs uitgeschreven door bureauhoofd ICT-Services.
- Men mag apparatuur die men meeneemt zoals laptops en elektronische agenda's niet onbeheerd achter laten. Gebruik de elektronische agenda alleen als agenda, adresboek en notitiemedium voor niet-vertrouwelijke informatie.
- Gebruikers van mobiele systemen en thuiswerkers moeten zelf zorgdragen dat ze van de gegevens van Gemeente Heerlen een back-up maken.
- Gebruikers van mobiele systemen en thuiswerkers moeten ervoor zorgen dat de toegang tot de vertrouwelijke informatie van Gemeente Heerlen die zich op hun systemen bevindt beperkt blijft tot hun zelf.

Recht op controle en onderzoek

Gemeente Heerlen mag alle informatie, zoals elektronische documenten, e-mail berichten, internetgedrag, op of over haar netwerk controleren. De directeur van Gemeente Heerlen behoudt zich dit recht om er zich van te verzekeren dat de gebruikers zich houden aan de beschreven normen en om de veiligheid van de computersystemen van Gemeente Heerlen te beschermen. Daarom moeten de gebruikers zich ervan bewust zijn dat ieder persoonlijk gebruik van de e-mail of internettoegang van Gemeente Heerlen kan worden gedetecteerd. We raden de gebruikers aan iedereen die hen wil e-mail berichten op het werk wil zenden op de hoogte te brengen van dit beleid.

D. richtlijnen

Verantwoordelijkheid i.v.m. wachtwoorden

Men mag wachtwoorden opschrijven op voorwaarde dat men het document fysisch beveiligt, bijvoorbeeld in een afgesloten kast.

2. Softwarelicenties en –gebruik

A. Doelgroep

1. De regeling geldt voor iedere medewerker die gebruik maakt van de telecommunicatiemiddelen van de gemeente Heerlen en die aan te merken is als ambtenaar in de zin van artikel 1:1 lid 1 sub a van de CAR alsmede voor uitzendkrachten, detacheringkrachten, stagiaires en personen die anderszins (betaald of onbetaald) werkzaamheden verrichten voor de gemeente Heerlen.
2. Voor de toepassing van deze regeling wordt onder telecommunicatiemiddelen verstaan:
telefoon, faxapparatuur, personal computer, overige communicatie- en informatietechnologische voorzieningen.

B. Doel

Alle werkplekken gekoppeld aan het netwerk van Gemeente Heerlen vallen onder verantwoordelijkheid van bureau ICT-Services. Eveneens de niet gekoppelde configuraties welke voorzien zijn van een identificatienummer van Gemeente Heerlen. Wijzigingen aan software- en hardwareconfiguraties kunnen het functioneren van het volledige netwerk van de gehele Gemeente Heerlen verstoren. In de doorberekeningmethodiek zijn alle kosten in verband met het verwerven, de ondersteuning en onderhoud van de ICT-diensten in opgenomen. We kunnen de kosten van de ICT-diensten van Gemeente Heerlen alleen controleren als alle gebruikers zich strikt onderwerpen aan het beleid en de procedures.

C. Verklaring

Alle software

- Het beleid van gemeente Heerlen staat alleen software toe waarvoor men een wettelijke licentie heeft. Alle software zal een licentie hebben op naam van Gemeente Heerlen en alleen medewerkers van bureau ICT-Services mag deze software installeren.
- Software zonder licenties / illegaal gekopieerde software is verboden op alle informatiesystemen van Gemeente Heerlen.

Gespecialiseerde software

Een afdeling die gespecialiseerde software nodig heeft, moet vooraf het bureauhoofd ICT-Services consulteren alvorens deze wordt aangeschaft. Om er zeker van te zijn dat dergelijke software past binnen de ICT-Architectuur van Gemeente Heerlen en op geen enkele manier in conflict is met de standaard software van de Gemeente Heerlen.

Verboden software

Het is verboden software te installeren bijvoorbeeld spelletjes, afwijkende schermbeveiligingen, eigen achtergrondschermen, systeemsoftware, internettools en hulpmiddelen om te kraken op elk systeem van Gemeente Heerlen.

Kopieën van software

Het is verboden om zelf kopieën van software van Gemeente Heerlen te maken, tenzij de licentieovereenkomst dit toelaat en de kopieën door de Helpdesk van bureau ICT-Services worden vervaardigd.

Privé-gebruik van software van Gemeente Heerlen

Software met een licentie op naam van Gemeente Heerlen mag men niet installeren op een computer die geen eigendom is van de Gemeente Heerlen.

3. Gedragsregels bij het gebruik van de Internet- en mail-voorziening van de Gemeente Heerlen

A. Doelgroep

1. De regeling geldt voor iedere medewerker die gebruik maakt van de telecommunicatiemiddelen van de gemeente Heerlen en die aan te merken is als ambtenaar in de zin van artikel 1:1 lid 1 sub a van de CAR alsmede voor uitzendkrachten, detacheringkrachten, stagiaires en personen die anderszins (betaald of onbetaald) werkzaamheden verrichten voor de gemeente Heerlen.
2. Voor de toepassing van deze regeling wordt onder telecommunicatiemiddelen verstaan:
telefoon, faxapparatuur, personal computer, overige communicatie- en informatietechnologische voorzieningen.

B. Doel

Het doel van deze normen is een richtlijn zijn voor alle gebruikers van de ICT-voorziening van Gemeente Heerlen in verband met het aanvaardbare gebruik en beveiliging van de Internet- en e-mailvoorziening van Gemeente Heerlen. Deze normen omvatten richtlijnen voor zowel over aanvaardbaar als onaanvaardbaar gebruik van Internet en e-mail, met de bedoeling het gedrag van de gebruikers en zijn handelingen die bijdragen tot risico's voor de Internet- en e-mailvoorziening van Gemeente Heerlen te controleren.

C. Verklaring

Viruspreventie en virusopsporing

Alle bestanden geladen van het Internet of ontvangen via de e-mailvoorziening worden voor gebruik gescreend met software voor virusbescherming. Dit geschiedt onder verantwoordelijkheid van bureau ICT-Services. De gebruiker moet de Helpdesk op de hoogte stellen van elke verdachte e-mailboodschap of bijlage.

De gebruikers moeten voorzichtig zijn met e-mailberichten en bijlagen van een onbekende bron, want virussen zitten vaak verborgen in bijlagen. Als men een virus vermoedt, mag men het verdachte bericht en bijlage niet openen of doorsturen. Men moet direct telefonisch contact opnemen met de Helpdesk van bureau ICT-Services.

Uitwisselen van informatie en transacties via Internet

De internetvoorziening van Gemeente Heerlen wordt ook gebruikt voor financiële transacties, koppelen van externe locaties met behulp van webtechnologie en plaatsen van bestellingen. De verhoogde beveiligingsvoorschriften moeten strikt gevolgd worden.

Elke boodschap die men meedeelt via Internet of per e-mail moet de naam van de afzender bevatten. Men mag geen e-mail of enige andere elektronische communicatie verzenden als ze de identiteit van de afzender verbergt of de afzender voorstelt als iemand anders. Geen enkele gebruiker mag de e-mail of internetvoorziening van een andere gebruiker gebruiken zonder voorafgaande toestemming van die gebruiker.

Men moet de voorgeschreven huisstijl hanteren en mag hier niet van afwijken.

Vertrouwelijkheid van informatie

Werknemers van Gemeente Heerlen mogen geen vertrouwelijke of privé-materiaal van Gemeente Heerlen versturen of publiceren tenzij de eigenaar van de informatie eerst de publicatie van dit materiaal goedgekeurd.

Opslaan van e-mailcommunicatie

Alle e-mailberichten moeten op de mailserver van Gemeente Heerlen worden opgeslagen waarop dagelijks een back-up wordt gemaakt. Het is niet toegestaan om zelf persoonlijke mappen (PST-file) aan te maken welke toestaan dat berichten anders dan de mailserver worden opgeslagen.

Gemeente Heerlen hanteert 2 standaarden met betrekking tot de opslagcapaciteit op de mailserver. De gebruiker dient zelf zorg te dragen voor opschoning van de e-mailberichten als de limietoverschrijding wordt aangekondigd.

4. Overeenstemming

Men verwacht van alle gebruikers dat ze hun gezond verstand gebruiken en op een professionele manier handelen in verband met het gebruik van de ICT-voorzieningen van Gemeente Heerlen. De gebruikers moeten zich ervan bewust zijn dat het zich niet houden aan deze normen kan leiden tot maatregelen afhankelijk van de aard van het vergrijp en het aantal overtredingen.

Gemeente Heerlen behoudt zich het recht voor de activiteiten op haar ICT-voorziening te controleren om het naleven van deze normen na te gaan. Gemeente Heerlen behoudt zich ook het recht voor, als ze dat nodig vindt, elke inbreuk op deze normen mee te delen aan de bevoegde beambten. Met inachtneming van hetgeen in de *Wet Beschermingspersoonsgegevens* is bepaald.

Het is de taak van de afdelingsverantwoordelijken het naleven van dit beleid en van elk ander beleid van Gemeente Heerlen.

Bureau ICT-Services zal het naleven van deze normen in alle aspecten van deze notitie controleren. Kleine inbreuken die voor het eerst plaatsvinden, zal men direct bespreken met de betrokken gebruiker. Herhaalde kleine inbreuken op het beleid en ernstige inbreuken die voor het eerst plaatsvinden, zal men rapporten aan de directeur voor verdere maatregelen.

5. Aanspreekpunten

Meer informatie en verduidelijking in verband met deze handleiding kunt u verkrijgen bij:

- Uw direct leidinggevende
- Afdeling P&O
- Bureauhoofd ICT-Services
- Helpdesk