REGLEMENT RELATIF A L'UTILISATION DES MOYENS DE COMMUNICATION ELECTRONIQUES, DU RESEAU INFORMATIQUE ET D'INTERNET AU SERVICE D'INCENDIE ET D'AIDE MEDICALE URGENTE - SIAMU

REGLEMENT BETREFFENDE HET GEBRUIK VAN DE ELEKTRONISCHE COMMUNICATIEMIDDELEN, HET INFORMATICANETWERK, INTERNET EN INTRANET IN BRUSSELSE HOOFDSTEDELIJKE DIENST VOOR BRANDWEER EN DRINGNDE MEDISCHE HULP

Table des matières – Inhoudstafel

1. Définitions

Art. 1 Pour l'application du présent règlement, on entend par :

Matériel informatique : tout composant matériel ou logiciel d'un poste de travail desservi au moyen d'un ordinateur, d'une tablette, d'un système tactile personnel ou multi-utilisateurs, relié ou non au réseau, en ce compris les matériels d'impression et de communication et leurs périphériques ainsi que tout moyen technique informatique ou bureautique mis en œuvre et visant une meilleure automatisation du travail.

Fichier : un ensemble de données, constitué et conservé suivant une structure logique devant permettre une consultation systématique.

Gestionnaire de réseau : l'IT manager en charge du bon fonctionnement du réseau informatique du Service d'Incendie et d'Aide Médicale Urgente de la Région de Bruxelles-Capitale SIAMU.

Données à « caractère personnel » : les données relatives à une personne physique identifiée ou identifiable.

Responsable du traitement : la personne physique ou morale, l'association de fait ou l'administration publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel conformément à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Prestataire externe : Toute personne détachée de son administration, de sa société ou service public d'origine et liée au SIAMU par une convention conclue entre son administration, son entreprise ou service public et le SIAMU.

1. Definities

Art. 1 Voor toepassing van onderhavig reglement worden verstaan onder:

Informaticamateriaal: elk materieel onderdeel of elke software van een werkpost bediend door een pc of een terminal voor meerdere gebruikers, al dan niet op het net aangesloten, met inbegrip van printers en communicatiemateriaal en hun afgeleiden alsook elk ingeschakelde technische ondersteuning inzake informatica of bureautica, bedoeld voor een betere automatisering van het werk.

Bestand: een geheel van gegevens samengesteld en bewaard volgens een logische structuur om een stelselmatige raadpleging mogelijk te maken.

Netbeheerder: IT manager bevoegd voor de goede werking van het informaticanetwerk van de Brusselse Hoofdstedelijke Dienst voor Brandweer en Dringende Medische Hulp - DBDMH.

Persoonsgegevens: iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

Verantwoordelijke voor de verwerking: de natuurlijke persoon of de rechtspersoon, de feitelijke vereniging of het openbaar bestuur die alleen of samen met anderen het doel en de middelen voor de verwerking van persoonsgegevens bepaalt in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

Externe prestatieverlener: elke persoon gedetacheerd van haar bestuur of oorspronkelijke overheidsdienst verbonden aan de DBDMH krachtens een conventie tussen haar/zijn bestuur of overheidsdienst met de DBDMH.

2. Champ d'application

Art. 2 Le présent règlement s'applique aux membres du personnel du SIAMU ainsi qu'aux prestataires externes qui utilisent le matériel informatique et/ou le réseau informatique du SIAMU.

2. Toepassingsgebied

Art. 2 Onderhavig reglement is van toepassing op de personeelsleden van DBDMH alsook op de externe prestatieverleners die gebruik maken van het informaticamateriaal en/of het informaticanetwerk van DBDMH.

3. Objet

Art. 3 Le présent règlement fixe les règles à respecter en ce qui concerne l'usage d'Internet, d'Intranet, des logiciels, du réseau informatique et des moyens de communication électronique ainsi que les finalités et les modalités de son contrôle dans le respect des garanties relatives à la protection de la vie privée des membres du personnel.

L'objectif est d'assurer un équilibre entre la protection de la vie privée des membres du personnel du SIAMU, utilisateurs d'Internet et des moyens de communication électroniques et la légitimité d'un contrôle de l'utilisation des outils électroniques et informatiques.

3. Voorwerp

Art. 3 Onderhavig reglement bepaalt de na te leven regels inzake de aanwending van internet en intranet, toepassingen, het informaticanetwerk en de elektronische communicatiemiddelen alsook de finaliteiten en modaliteiten van haar controle in naleving van de waarborgen inzake de bescherming van de persoonlijke levenssfeer van de personeelsleden.

De bedoeling is het evenwicht te verzekeren tussen de bescherming van de persoonlijke levenssfeer van de personeelsleden van de DBDMH, gebruikers van Internet en van de elektronische communicatiemiddelen en de legimiteit van een controle op het gebruik van elektronische informaticamateriaal.

4. Modalités générales d'utilisation et d'accès

4.1 Principe

Art. 4 Le SIAMU met à disposition des membres de son personnel des outils informatiques et électroniques de manière à permettre la réalisation des objectifs suivants :

- Faciliter la communication tant interne qu'externe,
- Offrir un outil de travail performant et adéquat dans le cadre des nouvelles technologies,
- Encourager l'apprentissage, l'utilisation et l'évolution de ces nouvelles technologies de manière à améliorer la qualité du travail presté et les compétences des membres du personnel dans ce domaine

Art. 5 Chaque membre du personnel est responsable de l'usage qu'il fait des outils électroniques et informatiques mis à sa disposition et les utilise en bon père de famille.

Art. 6 Seul l'usage à des fins professionnelles de ces outils est autorisé, c'est à dire un usage dédié exclusivement à l'exercice de la fonction dont le

4. Algemene gebruiks en toegangsmodaliteiten

4.1 Beginselen

Art. 4 De DBDMH stelt elektronica en informaticamateriaal ter beschikking van haar personeelsleden op een wijze die de realisatie van volgende doeleinden mogelijk maakt:

- de communicatie, zowel intern als extern, vlotter laten verlopen,
- Een performant en adequaat instrument aanbieden in het kader van de nieuwe technologieën
- Het leerproces, het gebruik en de evolutie van deze nieuwe technologieën aanmoedigen om de kwaliteit van het gepresteerde werk en de competenties van de personeelsleden in dit domein te verbeteren.

Art. 5 Elk personeelslid is verantwoordelijk voor het gebruik dat zij/hij maakt van de ter hare/zijne beschikking gestelde informatica en elektronicamateriaal en gebruikt deze als goede huisvader.

Art. 6 Enkel aanwending voor professioneel gebruik van dit materiaal is toegestaan, met andere woorden aanwending uitsluitend gewijd

membre du personnel est titulaire, sous réserve des précisions visées aux articles suivants.

Art. 7 Le gestionnaire du réseau crée pour chaque membre du personnel, lors de son entrée en fonction, un login associé à un mot de passe donnant accès au réseau informatique du SIAMU à partir d' ordinateurs reliés au réseau informatique par le biais d'une session individuelle, en ce compris l'accès à un compte de messagerie électronique professionnel, à l'Intranet et à l'Internet.

Le login et le mot de passe sont strictement confidentiels. Il est interdit de les communiquer à une autre personne, sauf exception.

Le login est fixe mais le mot de passe peut, à tout moment, être modifié unilatéralement et d'initiative par le membre du personnel par le biais de l'interface du login. Il est recommandé de modifier de temps en temps son mot de passe.

Il est interdit de se connecter sans autorisation à la session individuelle d'un autre utilisateur.

Lorsque l'utilisateur quitte son poste de travail et sait qu'il ne sera plus utilisé pendant plusieurs heures, il doit éteindre son poste. Lorsque l'utilisateur quitte son poste de travail temporairement, il doit soit le verrouiller (Ctrl+ alt+ del) afin de ne pas le laisser libre d'accès soit quitter sa session dans le cas de poste partagé.

Art. 8 Les membres du personnel doivent respecter le présent règlement et s'engagent à utiliser les outils informatiques et électroniques en bon père de famille, compte tenu des exigences de sécurité et de bon fonctionnement du réseau, notamment en matière de lutte contre la contamination du réseau par un virus ou tout malware.

L'utilisation des outils informatiques et électroniques mis à disposition par le SIAMU pour commettre des actes de criminalité informatique est interdite et pénalement réprimée.

aan de uitoefening van de functie waarvan het personeelslid titelhouder is, onder voorbehoud van verduidelijking in de hierna volgende artikelen.

Art. 7 De netbeheerder creëert voor elk personeelslid bij haar/zijn indiensttreding, een login en paswoord dat toegang verschaft tot het informaticanetwerk van de DBDMH vanaf om het even welke op het netwerk van de DBDMH aangesloten pc via een individuele sessie met inbegrip van toegang tot een professioneel elektronisch postvak tot internet en intranet.

De login en het paswoord zijn strikt vertrouwelijk. Het is verboden ze aan een andere persoon mede te delen, behalve bij uitzondering

De login is onveranderlijk maar het paswoord kan op elk moment eenzijdig en op initiatief van het personeelslid gewijzigd worden via de interface van de login. Het paswoord af en toe wijzigen wordt aanbevolen.

Het is verboden zich zonder toestemming aan te sluiten op de individuele sessie van een andere gebruiker.

Wanneer een gebruiker haar/zijn werkpost verlaat, en weet dat deze gedurende enkele uren niet meer zal gebruikt worden, moet de post uitgeschakeld worden. Wanneer een gebruiker haar/zijn werkpost tijdens de dagtaak tijdelijk verlaat, moet de post vergrendeld worden (Ctrl+ Alt+ Del) om de vrije toegang te verhinderen of moet de sessie afgesloten worden in geval van een gedeelde werkpost.

Art. 8 De personeelsleden moeten onderhavig reglement naleven en verbinden er zich toe de informatica en elektronicamateriaal als goede huisvader te behandelen met in achtneming van de verplichtingen inzake veiligheid en goede werking van het netwerk meer bepaald inzake de strijd tegen besmetting van het netwerk door virussen en andere malware.

Het gebruik van de door de DBDMH ter beschikking gestelde informatica en elektronisch materiaal voor daden van informaticacriminaliteit is verboden en wordt strafrechtelijk vervolgd.

4.2 Pour le personnel quittant le service temporairement (IDC, congé maternité, etc…)

Art 9 : Dans le cas où le membre du personnel quitte le service temporairement, l'agent est supposé être en congé et l'article 5.3 est d'application.
Son compte est temporairement bloqué et ses accès suspendus.
A titre exceptionnel et lorsque cela s'avère nécessaire en vue de la continuité du service, les fonctionnaires dirigeants peuvent décider de sursoir à cette fermeture temporaire.

4.2 Voor de medewerkers die de dienst tijdelijk verlaten (IDC, zwangerschapsverlof, enzovoort …).

Artikel 9: In het geval wanneer het personeelslid de dienst tijdelijk verlaat, wordt hij of zij beschouwd uit dienst te zijn en is paragraaf 5.3 van toepassing.
Zijn account wordt tijdelijk geblokkeerd en zijn toegang wordt tijdelijk ontzegd.
In uitzonderlijke omstandigheden en wanneer dat nodig is voor de continuïteit van de dienstverlening, kunnen leidinggevenden besluiten deze tijdelijke blokkering en ontzegging op te heffen.

5. Utilisation du compte de messagerie électronique

5.1 Principes

Art. 10 L'utilisation du compte de messagerie électronique est exclusivement professionnelle.

Art. 11 Le gestionnaire du réseau crée, pour chaque membre du personnel, un compte de messagerie électronique et une adresse de messagerie électronique sous la forme « xxx@firebru.irisnet.be».

Cette adresse de messagerie électronique permet d'identifier immédiatement la provenance du courrier électronique et la qualité de membre du personnel du SIAMU de son expéditeur.
Par l'envoi de courriers électroniques sortants, le membre du personnel est réputé représenter le SIAMU à l'égard des tiers.
Il veillera à respecter les obligations hiérarchiques et n'outre passera ses responsabilités au sein de l'organisation, c'est-à-dire sans être exhaustif:

- veillera à ne pas diffuser des informations non validées par son responsable hiérarchique
- s'assurera qu'il est bien autorisé à diffuser les informations (dans les cas de doute, validera avec sa hiérarchie)
- respectera les obligations de signature (pour les contrats, engagements du SIAMU …)

5. Gebruik van een elektronisch postvak

5.1 Beginselen

Art. 10 Het gebruik van het elektronisch postvak is uitsluitend professioneel.

Art. 11 De netbeheerder verschaft elk personeelslid een elektronisch postvak alsook een elektronisch postvakadres onder de vorm « xxx@firebru.irisnet.be ».

Door dit elektronisch postvak kan de oorsprong van de verzender van een elektronisch bericht onmiddellijk geïdentificeerd worden alsook het personeelslid van de DBDMH.
Door verzending van elektronische berichten wordt het personeelslid verondersteld ten overstaan van derden, de DBDMH te vertegenwoordigen.
Hij zal toezien op het respecteren van de hiërarchische verplichtingen en zijn bevoegdheden binnen de organisatie niet overschrijden. Dit betekent, zonder exhaustief te zijn :

- Erover waken geen informatie te verspreiden die niet gevalideerd is door zijn hiërarchische chef,
- Zich ervan vergewissen dat hij de toestemming heeft informatie te verspreiden (in geval van twijfel, gevalideerd met zijn hiërarchie),
- De verplichtingen inzake de

ondertekening respecteren (voor contracten, de BHDBDMH ergens toe verbinden…)

Art. 12 L'utilisation du compte de messagerie électronique professionnel créé par le SIAMU pour le membre du personnel doit être effectuée avec discernement et bonne foi.
Le membre du personnel est responsable de l'utilisation qu'il fait de son compte de messagerie électronique professionnel.
Même en cas de courriers électroniques entrants non désirés et contraires au présent règlement, le membre du personnel reste responsable de la conservation, de l'utilisation et/ou du transfert des courriers électroniques entrants.

Art. 12 Aanwending van het door de DBDMH voor het personeelslid gecreëerde elektronisch postvak gebeurt met gezond verstand en ter goede trouw.
Het personeelslid is verantwoordelijk voor het gebruik dat zij of hij maakt van haar of zijn professioneel elektronisch postvak.
Zelfs bij binnenkomende ongewenste of met onderhavig reglement onverenigbare berichten, blijft het personeelslid verantwoordelijk voor het opslaan, gebruik en of doorzenden van de binnenkomende elektronische berichten.

Art. 13 Pour des raisons techniques, le compte de messagerie électronique professionnel mis à disposition dispose d'une taille de stockage de 2GB maximum. Lorsque cette taille maximum est atteinte, un message automatique est transmis au membre du personnel qui doit immédiatement vider son compte de messagerie électronique.

Art. 13 Om technische redenen heeft het ter beschikking gestelde professionele elektronische postvak een maximum opslagcapaciteit van 2GB . Wanneer deze maximumcapaciteit bereikt is wordt er automatisch een bericht gezonden naar het personeelslid die dan onmiddellijk haar/zijn elektronisch postvak moet ledigen.

5.2 Obligations

Art. 14 Les membres du personnel doivent :

1° Consulter régulièrement leurs courriers électroniques entrants et y donner suite lorsqu'ils appellent une réponse ;

2° Rester vigilants et prudents quant au contenu des courriers électroniques sortants.

Pour rappel, le courrier électronique officiel est soumis aux mêmes dispositions que le courrier postal, l'enregistrement ainsi que les signatures doivent être respectées.

3° Effacer immédiatement le(s) courrier(s) électronique(s) reçu(s) qui serait contraires à une des dispositions du présent règlement et/ou prohibé(s) par la loi et le(s) signaler au gestionnaire du réseau ;

4° Si un expéditeur persiste dans l'envoi de courriers électroniques prohibés, le membre du personnel doit lui demander de cesser immédiatement ses envois, pour autant que l'expéditeur soit identifiable et que cette démarche soit possible, et en informer le gestionnaire du réseau.

5° Veiller à effacer au fur et à mesure les courriers électroniques traités, en vue de ne pas encombrer le système informatique. Si nécessaire, veiller à archiver et/ou classer ceux-ci.

6° Veiller à envoyer copie des courriers électroniques reçus aux personnes qui doivent être informées de ceux-ci, tout en évitant la multiplicité de ces envois.

7° Respecter l'ordre public, les bonnes mœurs, le droit à l'image, la vie privée et le secret de la correspondance.

5.2 Verplichtingen

Art. 14 De personeelsleden moeten:

1° Geregeld hun binnenkomende elektronische berichten raadplegen en reageren wanneer deze een antwoord vergen.

2° Waakzaamheid en voorzichtigheid in acht nemen inzake de inhoud van uitgaande elektronische berichten.

Ter herinnering, officiële elektronische post is inzake registratie en de handtekeningen onderhevig aan dezelfde voorschriften als traditionele poststukken. Deze moeten dus ook worden nageleefd.

3° De ontvangen elektronische berichten die tegen onderhavig reglement ingaan en of wettelijk verboden zijn onmiddellijk wissen en ze aan de netbeheerder melden.

4° Indien een verzender volhardt met het zenden van verboden elektronische berichten moet het personeelslid voor zover de verzender identificeerbaar is en deze aanpak mogelijk is, hem vragen onmiddellijk zijn zendingen stop te zetten en de netbeheerder inlichten.

5° Waken dat de afgehandelde elektronische berichten één na één uitgewist worden teneinde het informaticasysteem niet te overstelpen. Indien nodig deze berichten archiveren en/of klasseren.

6° Waken dat kopieën van de ontvangen elektronische berichten aan de personen die ervan ingelicht moeten worden verzonden worden, evenwel er op lettend dat hun aantal niet te groot is.

7° De openbare orde, de goede zeden, de beeldrechten, privacy en het briefgeheim respecteren opslaan, gebruik en of doorzenden van de binnenkomende elektronische berichten.

5.3 En cas d'absence

Art. 15 En cas d'absence de plus d'un jour, le membre du personnel administratif met en place une procédure de réponse automatique aux courriers électroniques entrants, mentionnant l'absence et sa durée ainsi que le nom et les

5.3 Ingeval van afwezigheid

Art. 15 Ingeval het personeelslid meer dan één dag afwezig is, activeert zij of hij de procedure voor automatisch antwoorden op de binnenkomende elektronische berichten met melding van de duur der afwezigheid en de

coordonnées de la personne de contact, membre du personnel du SIAMU, à laquelle l'expéditeur doit s'adresser.

Cette réponse automatique doit être rédigée en français et en néerlandais sur base du modèle mis à disposition par la direction.

Art. 16 Dans l'hypothèse où le membre du personnel n'a pu mettre en place lui-même une procédure de réponse automatique en cas d'absence de plus d'un jour conformément à l'article 15, il mandate une personne de confiance, membre du personnel du SIAMU, afin d'y procéder pour lui dans les plus brefs délais.

Art. 17 A titre exceptionnel et lorsque cela s'avère nécessaire en vue de la continuité du service, les fonctionnaires dirigeants peuvent décider de dévier les courriers électroniques entrants du membre du personnel absent vers un autre compte de messagerie électronique appartenant à un membre du personnel du SIAMU. Le membre du personnel concerné est informé sans délai de cette mesure.

gegevens van de contactpersoon, een personeelslid van de DBDMH, tot wie de verzender zich moet richten.

Dit automatisch antwoord moet in het Frans en het Nederlands opgesteld zijn op basis van het model ter beschikking gesteld door de directie marketing en ontwikkeling.

Art. 16 In de veronderstelling dat het personeelslid de procedure voor automatisch antwoorden zelf niet heeft kunnen activeren bij een afwezigheid van meer dan één dag zoals artikel 15 voorschrijft, mandateert zij of hij een vertrouwenspersoon, personeelslid van DBDMH, om dit zo spoedig mogelijk te doen.

Art. 17 Ten uitzonderlijke titel en wanneer de continuïteit van de dienst dit vereist, kunnen de leidende ambtenaren beslissen om de binnenkomende elektronische berichten van het afwezig personeelslid af te leiden naar een andere elektronisch postvak behorend tot een personeelslid van DBDMH. Het betrokken personeelslid wordt meteen ook ingelicht over deze maatregel.

5.4 Signature du courrier électronique

Art. 18 Chaque membre du personnel doit insérer à la fin de tout courrier électronique professionnel une signature en français et en néerlandais indiquant son identité, sa qualité et les coordonnées du SIAMU sur base du modèle mis à sa disposition.

5.4 Handtekening elektronisch bericht

Art. 18 Elk personeelslid moet op het einde van elk professioneel elektronisch bericht een handtekening in het Frans en in het Nederlands inlassen met haar of zijn identiteit en hoedanigheid en met de gegevens van de DBDMH, op basis van het model ter beschikking gesteld.

5.5 Interdictions

Art. 19 Il est interdit à tout membre du personnel, sans que cette liste ne soit exhaustive, de :

1° Accéder et/ou lire les courriers électroniques entrants adressés à autrui sauf accord préalable de l'intéressé (délégation dûment donnée).

2° Usurper l'identité ou le titre d'autrui en envoyant, à son insu ou en son nom, un courrier électronique.

3° Diffuser des données confidentielles et/ou personnelles concernant le SIAMU, les membres de son personnel ou ses partenaires et autorité de tutelle, sauf autorisation expresse ou nécessité dans le cadre strict de la conduite d'un dossier.

4° Echanger des messages personnels internes ou externes sans rapport avec la fonction (textes, blagues, images, vidéos…) vu les risques importants que cette pratique représente (blocage des lignes, propagation de malware…).

5° Charger et/ou lancer tout programme exécutable ou interprétable pouvant porter atteinte à la sécurité du système informatique et à l'intégrité des données du SIAMU. Seuls les logiciels régulièrement acquis par la direction informatique et justifiés en raison de la spécificité des traitements à assurer peuvent être chargés et exploités sur le système informatique du SIAMU par le gestionnaire du réseau. Les fichiers, programmes exécutables ou interprétables qu'un membre du personnel souhaiterait charger et/ou lancer devront être obligatoirement soumis, et ceci, préalablement à toute utilisation, au gestionnaire du réseau qui donnera, après vérification l'autorisation

5.5 Verbodsbepalingen

Art. 19 Volgende zaken zijn, zonder dat deze lijst exhaustief is, verboden voor elk personeelslid:

1° Zich toegang verschaffen tot, en/of lezen van elektronische berichten gericht aan iemand anders, behalve wanneer betrokkene vooraf ingestemd heeft (delegatie naar behoren verleend).

2° Zich de identiteit of de titel van iemand anders, met haar of zijn identiteit, aanmatigen buiten haar of zijn weten.

3° Vertrouwelijke en/of persoonlijke gegevens betreffende de DBDMH, personeelsleden of partners en voogdijoverheid verspreiden zonder uitdrukkelijke toestemming of noodzaak in het strikte kader van de vordering van een dossier.

4° Uitwisseling van persoonlijke berichten, intern of extern, zonder verband met de functie (teksten, moppen, beelden, video's, enzovoort) wegens groot risico dat deze handelingen vertegenwoordigen (blokkering lijnen, verspreiding malware, enzovoort).

5° Het laden of opstarten van elk uitvoerbaar of interpreteerbaar programma dat schade kan toebrengen aan het informaticasysteem en aan de integriteit van de gegevens van de DBDMH. Enkel de door de directie informatica correct aangekochte software, verantwoord omwille van de specificiteit van de te verzekeren verwerking, mag, door de netbeheerder geladen en geëxploiteerd worden op het informaticasysteem van DBDMH. Bestanden, uitvoerbare of interpreteerbare programma's die een personeelslid zou willen laden en/of opstarten moeten, vóór elk gebruik, aan de netbeheerder voorgelegd worden die, na verificatie, toelating of

ou le refus d'utilisation sans devoir le motiver.

6° Reproduire, diffuser, communiquer, sous quelque forme que ce soit, des informations susceptibles de porter atteinte à la dignité d'autrui, notamment l'envoi ou le transfert de courriers électroniques
, diffamatoires, racistes, révisionnistes, érotiques ou pornographiques, d'incitation à la discrimination, eu égard aux textes légaux applicables en la matière.

[1]7° Diffuser des données protégées par le droit d'auteur, le droit des producteurs bases de données, etc... , sauf après autorisation du titulaire du droit.

8° Diffuser des informations obtenues de manière illégale.

9° Utiliser le courrier électronique dans le cadre d'une activité professionnelle étrangère à la relation de travail liant le membre de personnel au SIAMU.

10° Diffuser des opinions personnelles en
les faisant passer pour celles du SIAMU.

weigering tot gebruik geeft zonder dit te moeten motiveren

6° De reproductie, verspreiding en communicatie onder om het even welke vorm van informatie die de waardigheid van anderen zou kunnen aantasten, meer bepaald het verzenden of doorzenden van eerrovende racistische, revisionistische, erotische of pornografische en tot discriminatie aanzettende mailberichten en dit de wettelijke teksten ter zake[2] van toepassing in acht nemend.

7° De verspreiding van door het de auteursrecht beschermde gegevens, rechten het recht op beeld, de privacy en het geheim der briefwisseling, naleven. van dbaseproducenten, enzovoort, behalve na toestemming van de titularis.

8° Verspreiding van informatie die illegaal bekomen werd.

9° Gebruik van de mailbox in het kader van een beroepsactiviteit die vreemd is aan de arbeidsverhouding die het personeelslid aan. DBDMH bindt.

10° Verspreiding van persoonlijke opinies en deze laten uitschijnen alsof ze van DBDMH zijn.

5.6 Utilisation du compte de messagerie à des fins privées

Art. 20 L'utilisation du compte messagerie du SIAMU à des fins privées est strictement interdite.

Art. 21 L'utilisation d'un webmail (compte de messagerie sur Internet type Hotmail, Skynet, Yahoo…) pour consulter ses messages électroniques privés est tolérée pour autant qu'elle reste raisonnable et qu'elle n'affecte pas l'exécution des tâches du membre du personnel et ce, dans les limites suivantes :

1° Ne pas entraver la bonne gestion du SIAMU, c'est à dire ne pas se faire au détriment des activités poursuivies par l'organisme ou de l'exécution des tâches du membre du personnel.

2° Ne pas constituer une infraction au présent règlement et ne pas contrevenir aux dispositions légales.

3° Ne pas engager la responsabilité du SIAMU.

4° Ne pas nuire à l'image du SIAMU.

5° Ne pas créer une confusion dans l'esprit des tiers quant aux identités et positions respectives du SIAMU et celles reprises dans le message du membre du personnel lui-même. A cet égard, il est important que soit exclue du courrier électronique toute indication qui pourrait laisser croire que le courrier électronique est rédigé dans le cadre de l'exercice de ses fonctions.

[1] Voyez notamment :
- la loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme et la xénophobie, la loi du 23 mars 1995 tendant à réprimer la négation, la minimisation, la justification ou l'approbation du génocide commis par le régime national socialiste allemand pendant la seconde guerre mondiale,
- les articles 383 et suivants du code pénal relatifs aux outrages publics aux bonnes mœurs, et notamment l'article 383 bis sanctionnant la diffusion ou la possession de documents à caractère pornographique concernant des mineurs d'âge,
- les articles 443 et suivants du code pénal sanctionnant les atteintes portées à l'honneur ou à la considération des personnes (calomnie, diffamation, injures,)…

5.6 Gebruik van een postvak van DBDMH voor privé doeleinden

Art. 20 Het gebruik van een postvak van DBDMH voor privé doeleinden is streng verboden.

Art. 21 Het gebruik van een webmail type (postvak op Internet, Hotmail, Skynet, Yahoo enzovoort) om private mails te raadplegen wordt gedoogd voor zover dit redelijk blijft en de uitvoering van de taken van het personeelslid niet aantast en dit binnen onderstaande perken:

1° Het goed beheer van de DBDMH niet hinderen met andere woorden niet ten koste van de activiteiten die de instelling verricht of de uitvoering der taken door het personeelslid.

2° Geen inbreuk vormen tegen onderhavig reglement en geen inbreuk plegen tegen de wettelijke beschikkingen.

3° De aansprakelijkheid van de DBDMH niet in gedrang brengen.

4° Het imago van de DBDMH niet beschadigen.

5° Geen verwarring scheppen in de geest van derden inzake de respectievelijke identiteiten en posities van de DBDMH en deze opgenomen in de mail van het personeelslid zelf. In dit verband is het belangrijk dat in elke mail aanwijzingen uitgesloten zijn die zouden kunnen laten voorkomen dat de mail opgemaakt werd in het kader van de uitoefening van haar of zijn functies

[2] Zie onder meer :
- Wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden, en de wet van 23 maart 1995 tot bestraffing van het ontkennen, [minimaliseren], rechtvaardigen of goedkeuren van de genocide die tijdens de tweede wereldoorlog door het Duitse nationaal-socialistische regime is gepleegd.
- De artikels 383 en volgende van het Strafwetboek betreffende openbare schennis van de goede zeden, meer bepaald artikel 383 bis ter bestraffing van het verspreiden of in bezit hebben van documenten met pornografisch karakter waarbij minderjarigen betrokken zijn.
- De artikels 443 en volgende van het Strafwetboek ter bestraffing van de aanranding van de eer of goede naam van personen (laster, eerroof, enzovoort).

6. Utilisation d'Internet

6.1 Principe

Art. 22 L'accès à Internet est fourni à des fins professionnelles.

Art. 23 Les fonctionnaires dirigeants se réservent le droit, sur proposition du gestionnaire de réseau, de bloquer à tout moment et sans avertissement préalable l'accès aux sites dont ils jugent le contenu illégal, offensant ou inapproprié dans le cadre professionnel, notamment lorsque la consultation des sites porte atteinte au bon fonctionnement du réseau ou à l'intérêt du service.

Dans tous les cas, les fonctionnaires dirigeants, sur proposition du gestionnaire du réseau, interdisent l'accès à des catégories de sites, tels que référencées par les fournisseurs d'Internet. Tout membre du personnel peut avoir copie de la liste des catégories dont l'accès est bloqué sur simple demande écrite adressée au gestionnaire de réseau.

Art. 24 La navigation sur Internet doit être effectuée avec discernement et bonne foi.

Art. 25 Le membre du personnel est seul responsable à l'égard du SIAMU et de tout tiers des sites qu'il consulte et sur lesquels il navigue, notamment lorsque le site requiert une identification.

6.2 Utilisation d'Internet à des fins privées

Art. 26 L'utilisation d'Internet à des fins privées est en principe interdite.

Art. 27 Elle est néanmoins tolérée pour autant qu'elle reste raisonnable et qu'elle n'affecte pas l'exécution des tâches du membre du personnel, dans ce cas, elle doit:

1° - être réalisée dans une optique d'apprentissage et de développement personnel ;

2° - être occasionnelle ;

3° ne pas entraver la bonne gestion du SIAMU, c'est à dire ne pas se faire au détriment des activités

6. Gebruik van internet

6.1 Beginsel

Art. 22 Toegang tot het internet wordt verschaft voor professionele doeleinden.

Art. 23 De leidende ambtenaren behouden zich het recht voor op voorstel van de netbeheerder op elk ogenblik en zonder voorafgaandelijke waarschuwing de toegang tot websites te blokkeren waarvan ze oordelen dat de inhoud illegaal, beledigend en ongepast is in de professionele context, meer bepaald wanneer raadpleging van bedoelde sites de goede werking van het netwerk of de belangen van de diensten aantast.

In elk geval verbieden de leidende ambtenaren op voorstel van de netbeheerder de toegang tot categorieën van sites zoals deze waar de internetleveranciers naar verwijzen. Elk personeelslid mag, op eenvoudig schriftelijk verzoek gericht aan de netbeheerder, kopie verkrijgen van de lijst der categorieën waarvan de toegang geblokkeerd is.

Art. 24 Surfen op het internet moet oordeelkundig en ter goeder trouw gebeuren.

Art. 25 Het personeelslid is alleen aansprakelijk ten aanzien van de DBDMH en elke derde voor de geraadpleegde sites waarop gesurft wordt, meer bepaald wanneer de site een identificatie vergt.

6.2 Gebruik van internet voor privé doeleinden

Art. 26 Het gebruik van internet voor privé doeleinden is in beginsel verboden.

Art. 27 Niettemin wordt dit gebruik gedoogd voor zover dit redelijk blijft en de uitvoering van de taken van het personeelslid niet verhindert en dit onder volgende voorwaarden:

1° gebruik in een optiek van bijleren en persoonlijke ontplooiing;

2° occasioneel ;

3° het goed beheer van de DBDMH niet hinderen met andere woorden niet ten koste van de

poursuivies par l'organisme ou de l'exécution des tâches du membre du personnel ;

activiteiten die de instelling verricht of de uitvoering der taken door het personeelslid;

4° ne pas constituer une infraction au présent règlement et ne pas contrevenir aux dispositions légales ;

4° geen inbreuk vormen tegen onderhavig reglement en geen inbreuk plegen tegen de wettelijke beschikkingen;

5° ne pas engager la responsabilité du SIAMU ;

5° de aansprakelijkheid van de DBDMH niet inzetten;

6° ne pas nuire à l'image du SIAMU et ne pas créer une confusion dans l'esprit des tiers quant aux identités et positions.

6° het imago van de DBDMH niet schaden en geen verwarring scheppen in de geest van derden inzake de identiteiten.

7° l'accès internet peut être limité pendant les heures de service.

7° De toegang tot het Internet kan beperkt worden tijdens de diensturen.

6.3 Interdictions

Art. 28 Les comportements suivants sont interdits, sans que cette liste soit exhaustive :

1° Utiliser des services sur Internet permettant l'échange d'idées et discussions en temps réel (chat, ou téléphonie par Internet tel Skype) ou différé (newsgroup), ainsi que des sites de type sociaux (netlog, facebook…) sauf si un tel accès est expressément autorisé par les fonctionnaires dirigeants lorsque l'intérêt du service le justifie.

2° Accéder à des sites d'achats en ligne pour compte du SIAMU sans autorisation préalable de l'organe compétent en vertu des délégations de signature en vigueur au SIAMU. En cas d'engagement de dépense au nom et pour compte du SIAMU sans autorisation préalable, le remboursement des sommes engagées sera demandé par le SIAMU, par voie judiciaire, le cas échéant, et une récupération sur salaire sera mise en œuvre.

3° Participer à la création d'un site ou utiliser le logo du SIAMU, sans autorisation expresse des fonctionnaires dirigeants.

4° Accéder à des sites où il est porté atteinte à la dignité d'autrui, eu égard aux textes légaux et réglementaires, et notamment ceux visés à l'article 19 6°, sans que cette liste ne soit exhaustive.

5° Accéder à des sites de jeux et paris, et de manière quelconque à tout site qui appartient à une catégorie de sites dont l'accès est bloqué sur ordre des fonctionnaires dirigeants.

6.3 Verbodsbepalingen

Art. 28 Volgend gedrag is verboden – deze lijst is niet exhaustief:

1° Internetdiensten gebruiken voor ideëenuitwisselingen en chatsessies in real time (chat, telefoneren via internet zoals bij Skype), of uitgestelde tijd (newsgroup), alsook voor sociale sites (Netlog, Facebook…), behalve wanneer dit uitdrukkelijk door de leidende ambtenaren toegelaten wordt wanneer het belang van de dienst dit rechtvaardigt.

2° Zonder instemming van de bevoegde instantie krachtens de in de DBDMH geldende handtekeningdelegaties naar websites surfen voor online aankopen (voor rekening) van de DBDMH. Ingeval van een aankoopverbintenis namens de DBDMH zal de DBDMH de terugbetaling van de overeengekomen bedragen vragen via gerechtelijke weg en desgevallend de terugbetaling op het salaris innen.

3° Zonder uitdrukkelijke toestemming van de leidende ambtenaren deelnemen aan de creatie van een website of het logo van de DBDMH

4° Naar websites surfen die de waardigheid van anderen aantast, de wettelijke en reglementaire teksten in achtnemend, meer bepaald deze bedoeld onder artikel 19 6°, zonder dat deze lijst exhaustief is welteverstaan.

5° Naar websites voor spelen en weddenschappen of naar om het even welke website surfen in de categorie van de op last van de leidende ambtenaren geblokkeerde sites.

7. Utilisation d'Intranet

Art. 29 Les informations placées par la (les) personne(s) autorisée(s) sur l'Intranet à l'attention des membres du personnel sont destinées à un usage interne.
Il est strictement interdit d'utiliser ces informations dans le cadre d'une communication externe vers des tiers sans accord préalable des fonctionnaires dirigeants.

7. Gebruik van Intranet

Art. 29 De op Intranet, door de daartoe bevoegde persoon of personen, geplaatste informatie voor de personeelsleden is enkel voor intern gebruik bedoeld.
Het is dus streng verboden deze informatie aan te wenden in het kader van externe communicatie naar derden.

8. Utilisation du Réseau

Art. 30 Le réseau informatique du SIAMU est réservé exclusivement à l'exercice de l'activité professionnelle et ne peut donc contenir que des fichiers, base de données et programmes nécessaires à l'accomplissement des missions du SIAMU.

Les fichiers qui y sont stockés sont considérés comme des fichiers professionnels.

Les fichiers personnels ne peuvent en aucun cas être stockés sur le réseau.

Art. 30bis – Un accès wifi à internet a été installé dans les salles de réunion. Ce réseau (SIAMU-DBDMH) est libre et gratuit. Il n'est pas contrôlé. En conséquence de quoi, il est formellement et rigoureusement interdit d'utiliser le réseau wifi simultanément avec la connexion câblée au réseau du SIAMU. L'accès à SIAMU-DBMH est autorisé uniquement lorsque le pc/laptop/smartphone n'est pas relié au réseau informatique du SIAMU. L'équipement devra préalablement être enregistré. Lorsque l'équipement est connecté, via un câble réseau, au réseau informatique du SIAMU, la connexion wifi doit obligatoirement être désactivée. L'utilisation du wifi se fait sous la seule responsabilité de l'utilisateur. Les articles 22 à 29 du présent règlement s'appliquent sans exception.

Art. 31 Chaque membre du personnel a accès à tout ou partie du réseau sur lequel doivent être sauvegardés tous les fichiers professionnels traités.

Art. 32 Un espace personnel est mis à disposition de chaque membre du personnel sur sa session sous la forme d'un « Personal Folder » (Y:/) afin d'y stocker, le cas échéant et de manière temporaire, des fichiers personnels.

La taille de cet espace est de 200 Mb maximum. En cas de dépassement de cette taille par les données stockées, un message automatique est généré invitant la personne concernée à vider/nettoyer son

8 Gebruik van het netwerk

Art. 30 - Het informaticanetwerk van de DBDMH is uitsluitend voorbehouden voor de uitoefening van de professionele activiteit en kan dus slechts bestanden, d-bases en programma's bevatten die noodzakelijk zijn voor het vervullen van de opdrachten van DBDMH.

De opgeslagen bestanden worden beschouwd als professionele bestanden.

Persoonlijke bestanden mogen dus in geen geval opgeslagen worden op het netwerk.

Art. 30bis – Er is een wifi-aansluiting tot het internet in de vergaderzalen geïnstalleerd. Dit netwerk (SIAMU-DBDMH) is vrij en kosteloos. Het wordt ook niet gecontroleerd. Ten gevolge hiervan is het uitdrukkelijk en streng verboden het wifi-netwerk tegelijkertijd te gebruiken met het kabelnetwerk van de DBDMH. De toegang tot SIAMU-DBMH is enkel toegelaten wanneer de pc/laptop/smartphone niet verbonden is met het informatisch netwerk van de DBDMH. Wanneer de hardware verbonden is, via een netwerkkabel, aan de informaticanetwerk van de DBDMH, moet de wifi-aansluiting verplicht uitgeschakeld worden. Aanwending van het wifi-netwerk gebeurt uitsluitend onder de verantwoordelijkheid van de gebruiker. De artikels 22 tot 29 van onderhavig reglement zijn thans zonder uitzondering van toepassing.

Art. 31 - Elk personeelslid heeft, volledige of gedeeltelijke toegang tot het netwerk waarin alle professioneel behandelde bestanden opgeslagen moeten worden.

Art. 32 - Voor elk personeelslid is er een persoonlijke plaats voorzien voor haar of zijn eigen postvak, in de vorm van « Personal Folder » (Y:/), bedoeld om desgevallend en tijdelijk, persoonlijke bestanden in op te slaan.

De omvang van deze ruimte is maximaal 200 Mb. Ingeval van overschrijding van deze omvang door de opgeslagen bestanden, komt er automatisch een bericht om het betrokken personeelslid te vragen

espace personnel.
Cet espace n'est pas destiné à stocker des données professionnelles. Chacun doit utiliser cet espace de manière raisonnable, avec discernement et bonne foi.

Il est à noter qu'un backup des fichiers personnels placés sur le (Y:/) n'est pas effectué. En cas de problème du système informatique, les fichiers seront perdus.

Art. 33 - Les fichiers professionnels doivent obligatoirement être placés sur le réseau de telle sorte à ce qu'ils soient disponibles pour toute personne concernée. Les fichiers doivent être classés selon les usages en vigueur.

haar of zijn persoonlijke plaats op te ruimen of leeg te maken. Deze ruimte is niet bedoeld om professionele gegevens in op te slaan. Iedereen moet deze ruimte op een redelijke manier en te goeder trouw gebruiken.

Te noteren: er wordt geen back-up verricht van de persoonlijke bestanden die op de (Y:/) zijn opgeslagen. Ingeval er zich informaticaproblemen voordoen zijn deze bestanden dan ook verloren.

Art. 33 - Professionele bestanden moeten op het netwerk geplaatst worden zodat ze voor elke betrokken persoon beschikbaar zijn. De bestanden worden geklasseerd volgens de van kracht zijnde normen.

9. Gestion et surveillance du système informatique par le gestionnaire du réseau

9.1 Mission

Art. 34 - Le gestionnaire du réseau exerce la gestion, la surveillance et l'analyse des flux d'informations entrants et sortants, et ce, dans un objectif de sécurisation du système informatique et du bon fonctionnement du réseau du SIAMU.

9.2 Mesures de prévention

Art. 35 - Le gestionnaire de réseau met en œuvre des mesures préventives visant à garantir la sécurité et l'intégrité du système informatique conformément aux finalités visées à l'article 44, ainsi :

- L'accès au réseau n'est autorisé qu'aux membres du personnel ou aux prestataires externes dûment identifiés ;
- Pour l'utilisation du réseau, le gestionnaire détermine, en fonction des besoins du service, quelles sont les ressources accessibles à chacun;
- Sont mis en place des logiciels qui visent à prévenir tout malware/risque d'intrusion sous quelque forme que ce soit et qui, à cette occasion, permettent de :
    - o Interdire le téléchargement de certains types de fichiers identifiés par leur format, soit parce qu'ils mobilisent sans motif lié à son activité les ressources du réseau, soit qu'ils sont susceptibles de faire courir un danger à la sécurité ou d'endommager les systèmes informatiques (par exemple : les fichiers de programmes exécutables) ;
    - o Limiter la taille des fichiers attachés en fonction des ressources du Réseau disponibles (bande passante, espace de stockage) ;
    - o Scanner les courriers électroniques

9. Beheer en bewaking van het informaticasysteem door de netbeheerder

9.1 Opdracht

Art. 34 - De netbeheerder oefent het beheer, de bewaking en de analyse uit van de binnenkomende en uitgaande informatiestromen en hij doet dit in een zorg om het informaticasysteem en de goede werking van het netwerk van de DBDMH veilig te stellen.

9.2 Preventiemaatregelen

Art. 35 - De netbeheerder neemt de preventieve maatregelen die de veiligheid en de integriteit van het informaticasysteem verzekeren overeenkomstig de finaliteiten onder artikel 44 alsook volgende bepalingen:

- De toegang tot het netwerk wordt enkel verleend aan personeelsleden en aan externe prestatieverleners die naar behoren geïdentificeerd zijn;
- Voor de toegang tot het netwerk bepaalt de netbeheerder, in functie van de behoeften in de dienst, welke bronnen voor elkeen toegankelijk zijn;
- De geïnstalleerde software is bedoeld om elke indringing van malware of ander risico, onder elke vorm ook, te voorkomen, en die, in voorkomend geval het volgende mogelijk maken:
    - o Verbod tot downloaden van sommige bestanden geïdentificeerd door hun formaat, hetzij omdat zij, zonder reden in verband met hun activiteit, de bronnen van het netwerk activeren, hetzij omdat zij in staat zijn de veiligheid in gevaar te brengen of het informaticasysteem te beschadigen (voorbeeld de bestanden van de uitvoerbare programma's);
    - o Beperking van de omvang van de bijgesloten bestanden in functie van de beschikbare netwerkbronnen (bandwijdte, opslagruimte);
    - o Scanning van binnenkomende mails om

entrants pour déterminer la présence d'un malware ;

o Supprimer certains courrier électroniques ou fichiers attachés sans préavis et sans prendre connaissance de leur contenu lorsque les systèmes de détection informatiques ont reconnu une menace pour la sécurité (Virus, spam, cheval de troie… tout malware quelconque) ;

Art. 36 - Le gestionnaire de réseau met en œuvre des logiciels permettant de prévenir des faits illicites, contraires aux bonnes mœurs ou à l'exécution de bonne foi du présent règlement ou portant atteinte à la dignité d'autrui, conformément aux finalités visées à l'article 44 et ainsi, permettre de:

- Repérer des sites suspects et, après décision des fonctionnaires dirigeants, bloquer l'accès aux sites Internet dont le contenu est illégal, offensant ou inapproprié;

- Supprimer sans préavis et sans prendre connaissance de leur contenu certains courriers électroniques ou fichiers non autorisés qui font l'objet d'une interdiction et/ou sont constitutifs d'une infraction pénale ;

Art. 37 La surveillance exercée par le gestionnaire du réseau via les mesures de prévention susvisées concerne exclusivement des données de trafic et non des données à caractère personnel et ce, dans l'intérêt du bon fonctionnement du système informatique.

Il s'agit d'une surveillance permanente, automatisée et non individualisée, n'ayant pas pour objet d'établir notamment un lien individuel entre les adresses des sites consultés ou les données transitant par le réseau et un membre du personnel en particulier.

La surveillance du trafic de données est réalisée dans le respect de la vie privée des membres du personnel ainsi que dans le respect du secret professionnel et de la confidentialité attachés aux données recueillies.

aanwezigheid van malware te bepalen;

o Schrapping van sommige mails of bijgesloten bestanden zonder bericht en zonder kennis te hebben genomen van hun inhoud wanneer het informaticadetectiesysteem een bedreiging voor de veiligheid ontwaard heeft (virussen, spams, Trojaanse paarden, of om het even welke malware);

Art. 36 - De netbeheerder installeert software die feiten voorkomt die ongeoorloofd zijn, in strijd zijn met de goede zeden of met de uitvoering ter goeder trouw van onderhavig reglement of de waardigheid van anderen aantast overeenkomstig de finaliteiten onder artikel 44 alsook volgende bepalingen mogelijk maakt:

- Verdachte websites opsporen en, na beslissing van de leidende ambtenaren, de toegang tot de websites met illegale, kwetsende of ongepaste inhoud blokkeren.

- Sommige mails of niet toegelaten bestanden die voorwerp zijn van verbod en of een strafrechtelijke inbreuk uitmaken, wissen, zonder voorafgaande kennisgeving en zonder kennis te nemen van de inhoud.

Art. 37 - De bewaking die de netbeheerder uitoefent via bovenbedoelde preventiemaatregelen behelst uitsluitend het gegevensverkeer en dus niet persoonsgegevens en dit in het belang van de goede werking van het informaticasysteem.

Het betreft een bestendige geautomatiseerde bewaking die niet geïndividualiseerd is en niet als voorwerp heeft bijvoorbeeld de individuele band te bepalen tussen de adressen van geraadpleegde websites of via het netwerk aangebrachte gegevens en een welbepaald personeelslid.

De bewaking van het gegevensverkeer gebeurt in naleving van de persoonlijke levenssfeer van de personeelsleden alsook met inachtneming van het beroepsgeheim en de vertrouwelijkheid verbonden aan de ontvangen gegevens.

La collecte des données est globale. Il s'agit d'apprécier le bon fonctionnement du réseau, d'Internet et des comptes de messagerie dans leur ensemble en disposant de l'accès aux informations relatives aux connexions à Internet (durée, date, heure, volumes, catégories et adresses des sites visités) et aux communications électroniques (volume, trafic…), sans individualisation de ces informations.

Het verzamelen van gegevens is globaal. Het gaat er om de goede werking van het netwerk, internet en de postvakken te beoordelen in hun geheel met de toegang ter beschikking tot de informatie betreffende de aansluitingen op internet (duur, datum, uur, volume, categorieën, adressen bezochte sites) en de mails (volume, verkeer, enzovoort), zonder individualisering van deze informatie.

Les logiciels utilisés agissent de manière programmée et automatique sur l'ensemble du trafic de données présentes sur le réseau sans que le gestionnaire du réseau ne prenne connaissance du contenu de ces données.

De gebruikte software werkt op geprogrammeerde en automatische wijze over het geheel van het gegevensverkeer in het netwerk zonder dat de netbeheerder kennis neemt van de inhoud van deze gegevens.

La confidentialité et la sécurité du traitement des données sont assurées.

Vertrouwelijkheid en beveiliging van de verwerking van deze gegevens zijn verzekerd.

Ce contrôle est inhérent et indispensable à la bonne gestion d'un système informatique.

Deze controle is eigen aan, alsook onontbeerlijk voor, een goed beheer van het informaticasysteem.

Art. 38 Les données sont stockées sur le serveur par le gestionnaire du réseau pendant une durée de trois mois maximum.

Art. 38 - De gegevens worden door de netbeheerder op de server opgeslagen gedurende een periode van 3 maanden maximum.

9.3 Interventions ponctuelles

Art. 39 En cas de problème d'ordre technique du système informatique quelle que soit son origine (réseau, Internet ou comptes de messagerie) laissant supposer que le problème provient d'une utilisation inadéquate ou abusive des outils informatiques, le gestionnaire du réseau peut examiner les caractéristiques des données susceptibles d'être à l'origine du problème en vue de résoudre le problème technique.

Si, pour ce faire, il doit individualiser la provenance des données, il en réfère au responsable de traitement et informe immédiatement le membre du personnel concerné de son intervention. Le gestionnaire du réseau ne peut pas prendre connaissance du contenu des données mais uniquement se baser sur des caractéristiques techniques telles que la taille, le type, l'extension, la quantité de fichiers attachés.

Art. 40 Le gestionnaire du réseau peut également localiser et récupérer des informations professionnelles essentielles qu'il est impossible d'obtenir par d'autres moyens (force majeure, …).

9.3 Gerichte tussenkomsten

Art. 39 ¬Ingeval van een probleem van technische aard in het informaticasysteem, ongeacht de oorsprong (netwerk, internet of postvak), dat laat veronderstellen dat het veroorzaakt is door inadequaat of ongerechtvaardigd gebruik van het informaticamateriaal, kan de netbeheerder, om het technisch probleem te kunnen oplossen, de kenmerken analyseren van de gegevens die in aanmerking komen als oorzaak van het probleem.

Indien hij om dit te doen de afkomst van de gegevens moet individualiseren, richt hij zich tot de verantwoordelijke voor de verwerking en licht hij onmiddellijk het betrokken personeelslid in over zijn tussenkomst. De netbeheerder mag geen kennis nemen van de inhoud van de gegevens maar moet zich uitsluitend op de technische kenmerken baseren zoals de grootte, het type, de uitbreiding en de hoeveelheid bijgesloten bestanden.

Art. 40 ¬De netbeheerder kan ook essentiële professionele informatie localiseren en opvragen wanneer het onmogelijk is ze op een andere wijze te bekomen (overmacht, enzovoort).

10. Traitement des données à caractère personnel

Art. 41 Le responsable du traitement des données à caractère personnel est le SIAMU, dont le siège social est sis 15 avenue de l'Héliport à 1000 Bruxelles et qui est représenté par les fonctionnaires dirigeants agissant conjointement.

Le responsable de traitement établit les finalités et les moyens du traitement des données à caractère personnel, qui ne peuvent être consignées que pour des objectifs nettement définis.

Le responsable de traitement peut confier à un « sous-traitant » le traitement des données à caractère personnel pour autant que le sous-traitant apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relative aux traitements et que le sous-traitant n'agisse que sur la seule instruction du responsable de traitement.
Le sous-traitant est tenu aux mêmes obligations que le responsable de traitement.

10. Verwerking persoonsgegevens

Art. 41 De verantwoordelijke voor de verwerking van persoonsgegevens is de DBDMH, met hoofdzetel Helihavanlaan 15 te 1000 Brussel en vertegenwoordigd door de leidende ambtenaren die samen optreden.

De verantwoordelijke voor de verwerking bepaalt de bedoeling en de middelen om persoonsgegevens te verwerken die slechts in bewaring kunnen gegeven worden voor duidelijk omschreven doelstellingen.
De verantwoordelijke voor de verwerking kan de verwerking van persoonsgegevens aan een "onderaannemer" toevertrouwen, voor zover de onderaannemer voldoende waarborgen geeft ten aanzien van de technische en organisatorische veiligheidsmaatregelen op het vlak van de verwerkingen en dat de onderaannemer slechts in opdracht van de verantwoordelijke voor de verwerking optreedt. De onderaannemer is door dezelfde verplichtingen als de verantwoordelijke

voor verwerking gebonden.

Le responsable de traitement ainsi que les personnes désignées sont tenues au secret professionnel.

De verantwoordelijke voor de verwerking alsook de aangestelde personen zijn gebonden door het beroepsgeheim.

Le Responsable de traitement adresse une déclaration à la Commission de la protection de la vie privée.

De verantwoordelijke voor de verwerking richt een verklaring aan de Commissie voor de bescherming van de persoonlijke levenssfeer.

11. Mesures de contrôle et d'individualisation

11.1 Principes et contrôle préventif

Art. 42 Les fonctionnaires dirigeants contrôlent le respect du présent règlement par les membres du personnel et ce, dans le respect des principes de finalité, de proportionnalité et de transparence ainsi que du droit au respect de la vie privée.

Art. 43 Les fonctionnaires dirigeants évaluent régulièrement la liste générale des sites consultés. Cette liste indique les sites, la durée et le moment des visites. Cette liste ne fait pas mention de l'identité des membres du personnel.
Ils peuvent, à l'occasion de ce contrôle général ou au départ d'autres sources d'information
lorsqu'ils constatent une anomalie, dans le cadre de la poursuite des finalités visées à l'article 44, sur proposition du gestionnaire de réseau:
-bloquer à tout moment et sans avertissement préalable l'accès aux sites dont le contenu est jugé illégal, offensant ou inapproprié dans le cadre professionnel,
-procéder à l'identification d'un membre du personnel, conformément à la procédure d'individualisation décrite ci-dessous.

Art. 44 Sur base d'indices généraux relatifs aux courriers électroniques tels la fréquence, le nombre, la taille, les annexes etc.…, certaines mesures de contrôle peuvent être prises par les fonctionnaires dirigeants vis à vis des messages, dans le cadre de la poursuite des finalités visées à
l'article 47. Si les fonctionnaires dirigeants présument un usage anormal ou interdit des courriers électroniques, ils procèdent, sur proposition du gestionnaire de réseau, à l'identification du membre du personnel concerné, dans le respect de la procédure d'individualisation décrite ci-dessous.

Art. 45 Dans les limites prévues par le présent règlement, le gestionnaire du réseau peut le cas échéant et sur ordre écrit du responsable de traitement individualiser les données collectées globalement, c'est à dire, les attribuer à un membre du personnel identifié ou identifiable.

11. Maatregelen ter controle en individualisering

11.1 Beginselen en preventieve controle

Art. 42 ¬De leidende ambtenaren controleren de naleving van onderhavig reglement door de personeelsleden en dit in naleving van de finaliteits en proportionaliteits en transparantie alsook van het recht op respect voor de persoonlijke levenssfeer.

Art. 43 ¬De leidende ambtenaren evalueren geregeld de algemene lijst der geraadpleegde websites. De lijst duidt de websites aan, de duur en het ogenblik van de raadpleging. Deze lijst maakt geen melding van de identiteit van de personeelsleden.
De leidende ambtenaren kunnen, bij zulke algemene controle of vanuit andere
informatiebronnen, wanneer ze iets abnormaals vaststellen, in het kader van de finaliteiten bedoeld onder artikel 44, op voorstel van de netbeheerder:
-op elk moment en zonder voorafgaande waarschuwing de toegang tot sites blokkeren waarvan de inhoud illegaal, kwetsend of ongepast is in het professionele kader,
-overgaan tot de identificatie van het personeelslid overeenkomstig de hierboven beschreven individualiseringsprocedure.

Art. 44 ¬Op basis van de algemene aanwijzingen betreffende mails, zoals de frequentie, het aantal, de omvang, de bijlagen enzovoort, kunnen de leidende ambtenaren sommige maatregelen nemen ten aanzien van deze mails in het kader van de naleving van de finaliteiten bedoeld onder artikel 47. Indien de leidende ambtenaren een abnormaal of ongeoorloofd gebruik van de mails vermoeden, gaan ze, op voorstel van de netbeheerder, over tot de identificatie van het betrokken personeelslid evenwel in naleving van de hierboven beschreven individualiseringsprocedure.

Art. 45 ¬Binnen de in onderhavig reglement voorziene perken kan de netbeheerder desgevallend en op schriftelijk verzoek van verantwoordelijke voor de verwerking de globaal verzamelde gegevens individualiseren, met andere woorden ze toeschrijven aan een geïdentificeerd of identificeerbaar personeelslid.

11.2 Finalités

Art. 46 Le SIAMU, représenté par ses fonctionnaires dirigeants, est autorisé à contrôler les données récoltées par le gestionnaire du réseau de manière globale et/ou individualisée, selon les procédures prévues par le présent règlement, lorsque l'une ou plusieurs des finalités suivantes est ou sont poursuivies.

Art. 47 Les finalités sont déterminées, explicites et légitimes au regard de l'intérêt :

1° La prévention de faits illicites, contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui : propos diffamatoires, données à caractère pornographique ou pédophile, faits incitant à la discrimination, à la ségrégation, à la haine ou à la violence selon la race, la couleur, l'ascendance, la religion, l'origine nationale ou ethnique, divulgation de fichiers ou de données confidentielles concernant par exemple la gestion du personnel ou des informations médicales, …

2° La protection des intérêts économiques, commerciaux et financiers du SIAMU auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires.

3° La sécurité et/ou le bon fonctionnement technique du système informatique en réseau du SIAMU, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations du SIAMU.

4° Le respect de bonne foi des règles et principes d'utilisation des technologies en réseau fixés par le présent règlement.

Les données recueillies doivent être adéquates, pertinentes et non excessives au regard des finalités fixées.

L'individualisation des données ne peut être requise qu'en cas de récurrence et si l'anomalie nécessite une identification du responsable.

11.2 Finaliteiten

Art. 46 De DBDMH vertegenwoordigd door de leidende ambtenaren is gemachtigd de gegevens die de netbeheerder globaal en/of geïndividualiseerd verzameld heeft te controleren volgens de procedures voorzien in onderhavig reglement wanneer een of meerdere van de onderstaande finaliteiten onderzocht worden.

Art. 47 De finaliteiten zijn, ten aanzien van het belang van de dienst bepaald.

1° De preventie van ongeoorloofde feiten, in strijd met de goede zeden en vatbaar om de waardigheid van anderen aan te tasten : eerrovende uitspraken, gegevens van pornografische of pedofiele strekking; volgens ras, huidskleur, afkomst, godsdienst, nationale of etnische afkomst tot discriminatie, segregatie, haat of tot geweld aanzettende feiten, ongeoorloofd verspreiden van vertrouwelijke gegevens en bestanden betreffende bijvoorbeeld het personeelsbeheer of medische informatie, enzovoort.

2° De bescherming van de economische, commerciële en financiële belangen van de DBDMH die een vertrouwelijk karakter hebben alsook de strijd tegen verkeerde praktijken.

3° De veiligheid en/of de goede technische werking van het informaticasysteem en het netwerk van de DBDMH, hierin begrepen de controle van de bijhorende onkosten alsook de fysieke bescherming van de inrichtingen van de DBDMH.

4° Ter goede trouw naleving van de regels en beginselen van het gebruik van de in het netwerk geïnstalleerde technologieën, door onderhavig reglement vastgelegd.

De opgevraagde gegevens moeten, ten aanzien van de vastgelegde finaliteiten, adequaat, relevant en niet overmatig zijn.

De individualisering van de gegevens mag slechts vereist zijn ingeval van herhaling en indien de anomalie een identificatie van de verantwoordelijke vergt.

11.3 Proportionnalité

Art 48 - Le traitement est limité par rapport au contenu des données, de manière à pouvoir identifier une personne.

Le SIAMU, responsable du traitement, garantit que les ingérences dans la vie privée des membres du personnel seront strictement limitées au contrôle organisé par le présent règlement et proportionnées au regard de la finalité poursuivie.

11.3 Proportionaliteit

Art. 48 - De behandeling is beperkt ten aanzien van de inhoud van de gegevens op een wijze een persoon te kunnen identificeren.

De DBDMH, verantwoordelijk voor de verwerking, verzekert dat inmenging in depersoonlijke levenssfeer van de personeelsleden strikt beperkt blijft tot de door onderhavig reglement georganiseerde controle, en in proportie is tot de gezochte finaliteit.

11.4 Modalités d'individualisation du contrôle

Art. 49 Par individualisation, on entend le traitement des données collectées lors d'un contrôle en vue de les attribuer à un membre du personnel identifié ou identifiable.

a) Individualisation directe sans avertissement préalable :

Art. 50 Le SIAMU, représenté par ses fonctionnaires dirigeants, procède, par ordre écrit adressé au gestionnaire du réseau, après proposition de celui-ci ou suite à d'autres sources d'information, à l'individualisation immédiate des données s'il suspecte ou constate :

- La commission de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;
- La violation des intérêts économiques et financiers du SIAMU, auxquels est attaché un caractère de confidentialité ;
- Une menace pour la sécurité et/ou le bon fonctionnement technique du système informatique en réseau du SIAMU, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations du SIAMU ;

11.4 Modaliteiten voor de individualisering van de controle

Art. 49 Onder individualisering wordt de verwerking van de verzamelde gegevens verstaan bij een controle om ze aan een geïdentificeerd of identificeerbaar personeelslid toe te schrijven.

a) Directe individualisering zonder voorafgaande waarschuwing

Art. 50 De DBDMH, vertegenwoordigd door de leidende ambtenaren; gaat, middels schriftelijk order aan de netbeheerder, na voorstel van deze laatste of gevolggevend aan andere informatiebronnen, over tot de directe individualisering van de gegevens wanneer zij het volgende verdenkt of vaststelt:

- Het begaan van ongeoorloofde of eerrovende feiten, feiten die in strijd zijn met de goede zeden of in aanmerking komen de waardigheid van anderen aan te tasten;
- De schending van de economische en financiële belangen van de DBDMH en belangen die omkleed zijn met vertrouwelijkheid;
- Een bedreiging voor de veiligheid en/of de goede technische werking van het informatienetwerk van de DBDMH met hierin ook begrepen de controle of de bijhorende onkosten alsook de fysieke bescherming van de inrichtingen van DBDMH ;

Dans ces cas, le SIAMU, représenté par les fonctionnaires dirigeants, peut identifier ou faire identifier le membre du personnel sans avertissement préalable.

Le membre du personnel est informé immédiatement de la mesure prise.

b) Individualisation indirecte

Art. 51 Hors les cas visés ci-dessus, un contrôle individuel, ponctuel et dûment justifié peut être effectué, dans les conditions suivantes si SIAMU, représenté par les fonctionnaires dirigeants, constate ou suspecte, sur base d'éléments probants, un manquement au principe de respect de bonne foi des règles et principes d'utilisation des technologies en réseau fixés par le présent règlement.

Toute personne qui constate un manquement au principe de respect de bonne foi des règles et principes d'utilisation des technologies en réseau fixés par le présent règlement en réfère aux fonctionnaires dirigeants.
Les fonctionnaires dirigeants prennent une décision motivée de mise sous surveillance temporaire de tout ou partie des membres du personnel, sans que ceux-ci ne soient identifiés personnellement. Pour cela, il faut des indices concordants laissant suspecter une utilisation incompatible des moyens de communication et/ou du réseau informatique.

Les fonctionnaires dirigeants informent tout ou partie des membres du personnel de la mesure de surveillance.

Le gestionnaire du réseau procède, pendant la durée de la surveillance à l'analyse des données de manière globale. S'il constate que l'anomalie se répète, il procède à l'individualisation des données.

Lors de cette individualisation, le gestionnaire du réseau peut être assisté d'un membre du personnel.

Le gestionnaire du réseau fait rapport aux fonctionnaires dirigeants.
Les fonctionnaires dirigeants informent le ou les membres du personnel concernés, procèdent éventuellement à une audition et prennent, le cas échéant une sanction.

In deze gevallen mag de DBDMH vertegenwoordigd door de leidende ambtenaren het personeelslid zonder voorafgaande waarschuwing identificeren.

Het personeelslid wordt onmiddellijk over de genomen maatregel ingelicht.

b) Indirecte individualisering

Art. 51 Behalve de hierboven bedoelde gevallen kan een individuele, gerichte en naar behoren gerechtvaardigde controle plaatsvinden onder volgende voorwaarden, indien de DBDMH, vertegenwoordigd door de leidende ambtenaren, op basis van overtuigende elementen een inbreuk vaststelt of vermoedt tegen het beginsel van ter goede trouw naleving inzake regels en gebruiksprincipes van de netwerktechnologieën bepaald in onderhavig reglement.

Elke betrokken persoon die een inbreuk vaststelt tegen het beginsel van ter goede trouw naleving inzake regels en gebruiksprincipes van de netwerktechnologieën bepaald in onderhavig reglement, wendt zich tot de leidende ambtenaren.
De leidende ambtenaren nemen een gemotiveerde beslissing om tijdelijk personeelsleden of een deel ervan, in het oog te houden zonder dat deze persoonlijk geïdentificeerd zijn. Samenhangende aanwijzingen zijn nodig om onverenigbaar gebruik te vermoeden van de communicatiemiddelen of het informaticanetwerk.

De leidende ambtenaren waarschuwen de personeelseden of een deel ervan betreffende de bewakingsmaatregel.

De netwerkbeheerder verricht tijdens de gehele duur van het toezicht, op globale wijze een analyse van de gegevens. Wanneer hij vaststelt dat de anomalie zich herhaalt, gaat hij over tot de individualisering van de gegevens.

Bij deze individualisering kan de netwerkbeheerder bijgestaan worden door een personeelslid.
De netbeheerder brengt verslag uit bij de leidende ambtenaren.
De leidende ambtenaren lichten het personeelslid of de personeelsleden in, gaan gebeurlijk over tot een verhoor en sanctioneren desgevallend.

12. Communication

Art. 52 Les fonctionnaires dirigeants veillent à informer les membres du personnel des mesures de surveillance qui sont mises en œuvre, à leur demande, par le gestionnaire du réseau.

Dans tous les cas, chaque membre du personnel est informé :

- de l'identité du gestionnaire de réseau ;
- de l'identité du responsable de traitement
- des données à caractère personnel ;
- que des données globales sont collectées par le gestionnaire du réseau ;
- du contenu du présent règlement et des consignes d'utilisation du système informatique (PC, Internet, Intranet, courriers électroniques). Si nécessaire un code de bonne pratique est édité et mis à disposition via l'Intranet.

Chaque membre du personnel peut s'adresser au service informatique en cas de difficulté dans la compréhension et l'application des principes du présent règlement.

12. Communicatie

Art. 52 ¬De leidende ambtenaren waken erover dat de personeelsleden ingelicht worden over de bewakingsmaatregelen die de netbeheerder op hun verzoek uitvoert.

Elk personeelslid wordt ingelicht over:

- de identiteit van de netbeheerder;
- de identiteit van de verantwoordelijke van de verwerking der persoonsgegevens;
- het feit dat de globale gegevens verzameld worden door de netbeheerder;
- over de inhoud van onderhavig reglement en de richtlijnen voor het gebruik van het informaticasysteem (pc, internet, intranet, mails). Indien nodig wordt er een code voor goede praktijk uitgevaardigd en ter beschikking gesteld via Intranet.

Elk personeelslid mag zich tot de informatica dienst richten ingeval van problemen bij het begrip en de toepassing van de beginselen van onderhavig reglement.

13. Droits des membres du personnel par rapport à ses données personnelles

Art. 53 Les membres du personnel ont le droit de prendre connaissance de toute information les concernant ayant fait l'objet d'un enregistrement par le gestionnaire de réseau. Ils ont le droit de recevoir une copie des données enregistrées dans un délai d'un mois après en avoir formulé la demande écrite auprès du responsable de traitement soit, au SIAMU, à l'attention des fonctionnaires dirigeants.

Les membres du personnel ont le droit d'obtenir la rectification de toute donnée enregistrée inexacte les concernant.

Les membres du personnel ont le droit d'obtenir la suppression ou l'interdiction d'utilisation de toute donnée à caractère personnel enregistrée les concernant qui, compte tenu des finalités du

13. Rechten van de personeelsleden ten aanzien van hun persoonlijke gegevens

Art. 53 ¬De personeelsleden hebben het recht kennis te nemen van elke informatie die hen aangaat en die voorwerp was van een registratie door de netbeheerder. Zij hebben recht kopie te ontvangen van de geregistreerde gegevens binnen de wachttijd van 1 maand na er schriftelijk om gevraagd te hebben hetzij bij de verantwoordelijke voor de verwerking, hetzij bij de DBDMH, ter attentie van de leidende ambtenaren.

De personeelsleden hebben het recht om de rectificatie van elke onjuist geregistreerd gegeven dat hen aangaat

De personeelsleden hebben recht om de schrapping of het verbod op gebruik te bekomen van elk geregistreerd persoonsgegeven dat hen aangaat en dat, gelet op de

traitement, est inexacte, incomplète ou dont l'enregistrement, la communication ou la conservation sont légalement interdits ou qui a été conservée au delà d'une période raisonnable, prenant fin un an après la fin des relations de travail entre les parties.

verwerkingsfinaliteiten, onjuist of onvolledig is of waarvan het opslaan, de communicatie of bewaring wettelijk verboden is of dat bewaard werd meer dan een jaar na het eind van de arbeidsverhouding tussen partijen.

Pour exercer les droits visés aux alinéas 2 et 3, le membre du personnel adresse une demande datée et signée au responsable du traitement soit, au SIAMU, à l'attention des fonctionnaires dirigeants. Dans le mois qui suit l'introduction de la demande écrite, le SIAMU communiquera les rectifications ou effacement de données à la personne concernée.

Om de in de 2de en 3de alinea beoogde rechten uit te oefenen, richt het personeelslid een gedagtekend en ondertekend verzoek tot de verantwoordelijke voor de verwerking, hetzij tot de DBDMH, ter attentie van de leidende ambtenaren. Binnen de maand volgend op het indienen van het schriftelijk verzoek, deelt de DBDMH de gegevensrechtzettingen of schrappingen aan de betrokken persoon mede.

14. Sanctions

Art. 54 Le non-respect du présent règlement est susceptible de donner lieu à l'une des sanctions suivantes, en fonction de la gravité du manquement en cause :

1° Avertissement écrit reprenant le fait reproché.

2° Retrait de l'utilisation du compte de messagerie électronique ou de l'accès à Internet, soit temporairement, soit définitivement.

Ces mesures peuvent être appliquées sans préjudice des autres sanctions prévues par les dispositions applicables en matière disciplinaire aux membres du personnel statutaires par l'arrêté du Gouvernement de la Région de Bruxelles Capitale du 26 septembre 2002 portant le statut administratif et pécuniaire des agents des organismes d'intérêt public de la Région de Bruxelles Capitale ou en matière de licenciement aux membres du personnel contractuels par l'arrêté du Gouvernement de la Région de Bruxelles Capitale du 20 juillet 2006 réglant la situation administrative et pécuniaire des contractuels des organismes d'intérêt public de la Région de Bruxelles de Capitale et la loi du 3 juillet 1978 relative aux contrats de travail

En effet, l'auteur de comportements interdits par le présent règlement, le cas échéant, réprimés et érigés en infractions par la loi, s'expose au licenciement pour faute grave, à une sanction disciplinaire ou à toute autre mesure, en fonction de la gravité de son comportement.

Ces mesures ne font pas obstacle à la mise en cause devant les juridictions compétentes de la responsabilité civile et/ou pénale de la personne concernée.

14. Sancties

Art. 54 Niet naleving van onderhavig reglement kan aanleiding geven tot volgende sancties, in functie van de ernst van het gebrek in kwestie:

1° Schriftelijke waarschuwing betreffende het aangeklaagde feit.

2° Intrekking van het gebruik van een elektronisch postvak of van de toegang tot internet, hetzij tijdelijk, hetzij definitief.

Deze maatregelen kunnen toegepast worden zonder nadeel der ander sancties die voorzien zijn door de beschikkingen die van toepassing zijn inzake tuchtsancties voor het statutair personeel door het besluit van de Brusselse Hoofdstedelijke Regering van 26 september 2002 houdende het administratief statuut en de bezoldigingsregeling van de ambtenaren van de instellingen van openbaar nut van het Brussels Hoofdstedelijk Gewest of inzake ontslag voor het contractueel personeel door het besluit van de Brusselse Hoofdstedelijke Regering van 20 juli 2006 tot regeling van de administratieve en geldelijke toestand van de contractuele personeelsleden van instellingen van openbaar nut van het Brussels Hoofdstedelijk Gewest en de wet van 3 juli 1978 betreffende de arbeidsovereenkomsten.

De dader van door dit reglement ongeoorloofd gedrag, dat desgevallend door de wet beteugeld en als inbreuk uitgevaardigd is, stelt zich bloot aan ontslag wegens zware fout, aan een tuchtsanctie of aan elke andere maatregel, in functie van de ernst van haar of zijn gedrag.

Deze maatregelen zijn geen beletsel tot betwisting bij de bevoegde jurisdicties voor de burgerlijke en/of strafrechtelijke aansprakelijkheid van de betrokken persoon.

15. Evaluation du contrôle

Art. 55 Les systèmes de contrôle installés font l'objet d'une évaluation régulière en Comité de concertation de base, notamment eu égard à leur révision en fonction des développements technologiques.

15. Evaluatie van de controle

Art. 55 ¬De geïnstalleerde controlesystemen zijn voorwerp van geregelde evaluatie door het Basisoverlegcomité, meer bepaald de inachtneming van hun revisie in functie van de technologische ontwikkelingen.

16. Helpdesk

Art. 56 Chaque membre du personnel peut contacter le service helpdesk , pour des questions techniques concernant le matériel informatique et son fonctionnement ou l'expression de besoins nouveaux via:
- le système de gestion de ticket "Helpdesk"
- l'adresse HelpDesk@firebru.irisnet.be.

16. Helpdesk

Art. 56 Voor technische vragen inzake informaticamateriaal of de werking ervan, of voor het formuleren van nieuwe noden, kan elk personeelslid de helpdeskdiensten raadplegen via

- het systeem voor het beheer van de ticketten "Helpdesk"
- het e-mailadres HelpDesk@firebru.irisnet.be

17. Entrée en vigueur

Art. 57 Le présent règlement entre en vigueur à compter du **30 mai 2014.**

17. Inwerkingstreding

Art. 57 ¬Onderhavig reglement wordt van kracht vanaf **30 mei 2014**.

18. Publicité

Art. 58 Le présent règlement est affiché aux valves et disponible à la GRH et sur l'Intranet. Il est également communiqué directement aux membres du personnel.

18. Bekendmaking

Art. 58 ¬Onderhavig reglement wordt ad valvas bekend gemaakt, is beschikbaar bij het HRMX en via intranet en wordt ook rechtstreeks aan de personeelsleden overgemaakt.

La Directrice Générale

Chantal Jordan

Le Directeur Général Adjoint

Johan Schoups