# ANNEXE 11 – Charte relative à l'utilisation des OUTILS INFORMATIQUES mis à disposition du personnel de Bruxelles Environnement - IBGE

**PREAMBULE :**

La présente instruction a été rédigée, dans le souci d'utiliser les moyens de communication disponibles à Bruxelles Environnement - IBGE, et notamment l'accès à Internet et l'usage du courriel, dans le respect de la loi, ainsi que des droits de l'homme et libertés fondamentales, sur base des dispositions suivantes :

- La Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, et notamment l'article 8.
- La Directive 95/46/CE du parlement européen et du conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données.
- La Constitution, et notamment l'article 22.
- La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel modifiée par la loi du 11 décembre 1998, et notamment son article 16 § 3 qui fait obligation de garantir la sécurité des données à caractère personnel récoltées et conservées par le maître de fichier, par toute mesure technique et organisationnelle requise pour protéger les fichiers qu'il gère.
- La loi du 21 mars 1991 portant réforme de certaines entreprises publiques autonomes qui interdit la prise de connaissance par un tiers de données transmises par voie de télécommunication, et notamment l'article 109 ter D.
- Le code pénal, et notamment l'article 314 bis qui réprime l'écoute, la prise de connaissance et l'enregistrement pendant leur transmission des communications ou télécommunications privées, sans le consentement de tous les participants concernés.
- La responsabilité en tant que maître de fichier.
- L'avis n° 10/2000 du 3 avril 2000 de la Commission de la protection de la vie privée.

La mise à disposition des outils de communication par Bruxelles Environnement - IBGE au personnel de l'organisme est sous-tendue par les 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 de travail presté et les compétences du personnel dans ce domaine.

60 Debaets rép-Annexe1 FR.doc

**ARTICLE 1 : CHAMP D'APPLICATION**

La présente instruction s'applique à l'ensemble du personnel de Bruxelles Environnement - IBGE, qu'il s'agisse d'agents statutaires, contractuels administratifs ou pédagogiques, ou autres, à quel que titre que ce soit, dans la mesure où il existe un lien de subordination entre l'agent et l'organisme.

**ARTICLE 2 : DROIT DE PROPRIETE**

Le matériel mis à disposition du personnel sur son lieu de travail, même occasionnel, appartient à Bruxelles Environnement - IBGE.

**ARTICLE 3 : MODALITES D'UTILISATION ET D'ACCES**

Toute personne, qui dispose d'un accès aux systèmes d'information l'utilise à des fins professionnelles, c'est-à-dire dans le cadre de l'exercice de ses fonctions.

Elle est responsable de l'usage qu'elle fait de ces systèmes d'information et les utilise en bon père de famille.

En outre, l'utilisation et l'accès doivent être pratiqués, compte tenu des exigences de sécurité et de bon fonctionnement des systèmes, en vue de les protéger contre les risques, tels que la contamination de virus ou l'intrusion.

A cet effet, Bruxelles Environnement - IBGE met à disposition les moyens nécessaires à la sécurisation des accès aux dits systèmes.

Il est interdit de se connecter sans autorisation au compte (mail ou réseau) d'un collègue qu'il soit présent ou non, et d'utiliser son compte afin d'envoyer des messages non tolérés. Soyez prudent avec votre mot de passe et modifiez-le régulièrement.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leurs sont propres (MyDocuments), et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées. Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie.

Recommandations :

- Chaque utilisateur doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater
- Chaque utilisateur doit faire la demande via le helpdesk pour toute installation de logiciel.

  **Comment faire ?**
  **Ouvrir un Ticket via GLPI (voir intranet ou raccourci dans START)**
  **Tél : 990**
  Mail : helpdeskict@ibgebim.be

- Chaque utilisateur doit s'engager à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers le matériel dont il a l'usage.
- Lorsque l'utilisateur quitte son poste de travail, il veille à le verrouiller (Ctrl+alt+del) pour ne pas le laisser en libre-service.

**ARTICLE 4 : REGLES SPECIFIQUES A L'UTILISATION DU COURRIEL**

- Le courriel doit être utilisé avec discernement.

- Les messages prohibés par la loi que risque de recevoir le membre du personnel de l'organisme doivent faire l'objet d'un effacement immédiat. Le membre du personnel n'est pas responsable du contenu des messages qu'il reçoit, mais peut être considéré comme responsable de l'utilisation ou du transfert des messages reçus. Si l'expéditeur persiste dans l'envoi de tels courriers, 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.

L'utilisation du courriel à des fins privées est tolérée, aux conditions suivantes :

- ✓ ne pas entraver la bonne gestion de Bruxelles Environnement - IBGE, c'est-à-dire ne pas se faire au détriment des activités poursuivies par l'organisme ;

- ✓ ne pas constituer une infraction à la présente instruction et ne pas contrevenir aux dispositions légales ;

- ✓ ne pas engager la responsabilité de Bruxelles Environnement - IBGE ;

- ✓ ne pas nuire à l'image de l'organisme et ne pas créer une confusion dans l'esprit des tiers quant aux identités et positions respectives de Bruxelles Environnement - IBGE et celles reprises dans le message du membre du personnel lui-même. A cet égard, il est important que soit exclue du message toute indication qui pourrait laisser croire que le message est rédigé dans le cadre de l'exercice de ses fonctions.

Les comportements suivants sont interdits :

- ✘ inviter ou participer à une chaîne de lettres sans utilité sociale;

- ✘ diffuser des données confidentielles $^{et}/_{ou}$ personnelles concernant l'organisme, son personnel, ses stagiaires ou ses partenaires, sauf autorisation expresse des titulaires du droit ou exception prévue par la loi ;

- ✘ reproduire, diffuser, communiquer, sous quelque forme que ce soit, des informations susceptibles de porter atteinte à la dignité d'autrui, eu égard aux textes légaux et réglementaires, et notamment, sans que cette liste soit exhaustive :

  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, chapitre V, sanctionnant les atteintes portées à l'honneur ou à la considération des personnes (calomnie, diffamation, injures,)…

  - dont le contenu est jugé illicite (publications interdites par la loi ou non légalement accessibles) ou préjudiciable à un tiers : - à caractère pornographique ;
    - sans son autorisation préalable.

  - usurper l'identité ou le titre d'autrui en diffusant à son insu $^{et}/_{ou}$ en son nom un courriel ;

  - diffuser des données protégées par le droit d'auteur, le droit des producteurs de bases de données, …, sauf autorisation du titulaire du droit ;

  - diffuser des informations obtenues de manière illégale ;

  - utiliser le courriel dans le cadre d'une activité professionnelle étrangère à la relation de travail ;

Enfin, il y a lieu de respecter l'ordre public, les bonnes mœurs, le droit à l'image, la vie privée, le secret de la correspondance.

Dans le respect de la confidentialité des communications, il est interdit d'essayer d'accéder ou de lire les messages électroniques d'autrui sauf accord préalable de l'intéressé (délégation dûment donnée).

Recommandations :

- Chaque utilisateur consulte régulièrement son courrier entrant, donne suite aux messages qui appellent une réponse.
- Chaque utilisateur veille à effacer au fur et à mesure les messages traités, en vue de ne pas encombrer le système informatique. Si nécessaire, il veille à l'archivage ou au classement de certains messages. Dans ce cadre certains outils sont et seront mis en place. Les formations nécessaires seront également organisées.
- Chaque utilisateur veille à envoyer copie des messages reçus aux personnes qui doivent être informées de ceux-ci, tout en évitant la multiplicité de ces envois.
- En cas d'absence prolongée, il est recommandé d'en informer ses correspondants en installant sur sa messagerie une réponse automatique d'absence mentionnant la durée de celle-ci et le nom, ainsi que les coordonnées d'une personne à qui il y a lieu de s'adresser en cas d'urgence.
- Chaque utilisateur est tenu à la plus grande prudence quant au contenu des messages qu'il envoie. En cas de participation à un forum à titre privé, il est tenu de mentionner que le message reflète ses seules opinions personnelles.
- En cas d'inscription à des forums ou des réseaux sociaux à caractère privé l'utilisation de l'adresse e-mail professionnelle est proscrite. Il est recommandé dans ce cas d'utiliser son adresse e-mail privée.

**ARTICLE 5 : REGLES SPECIFIQUES A L'UTILISATION DE L'INTRANET**

Les comportements suivants sont interdits :

- ✘ reproduire, diffuser, communiquer, sous quelque forme que ce soit, des informations susceptibles de porter atteinte à la dignité d'autrui, eu égard aux textes légaux et réglementaires, et notamment, sans que cette liste soit exhaustive :

  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, chapitre V, sanctionnant les atteintes portées à l'honneur ou à la considération des personnes (calomnie, diffamation, injures,)…

  - dont le contenu est jugé illicite (publications interdites par la loi ou non légalement accessibles) ou préjudiciable à un tiers : - à caractère pornographique ;
    - sans son autorisation préalable.
  - usurper l'identité ou le titre d'autrui ;
  - diffuser des données protégées par le droit d'auteur, le droit des producteurs de bases de données, …, sauf autorisation du titulaire du droit ;
  - diffuser des informations obtenues de manière illégale ;

Enfin, il y a lieu de respecter l'ordre public, les bonnes mœurs, le droit à l'image, la vie privée, le secret de la correspondance.

**ARTICLE 6 : REGLES SPECIFIQUES A LA NAVIGATION SUR INTERNET**

Lors de la navigation sur Internet, chacun doit être particulièrement attentif aux sites dont l'accès est conditionné par l'identification de l'internaute. Dans ce cas, il s'engage seul.

Pour le personnel disposant d'un accès à Internet, l'usage d'Internet à des fins privées est toléré aux conditions suivantes :

- ✓ être réalisé dans une optique d'apprentissage et de développement personnel ;
- ✓ être occasionnel ;
- ✓ ne pas entraver la bonne gestion de Bruxelles Environnement - IBGE, c'est-à-dire ne pas se faire au détriment des activités poursuivies par l'organisme ;
- ✓ ne pas constituer une infraction à la présente instruction et ne pas contrevenir aux dispositions légales ;
- ✓ ne pas engager la responsabilité de Bruxelles Environnement - IBGE ;
- ✓ ne pas nuire à l'image de l'organisme et ne pas créer une confusion dans l'esprit des tiers quant aux identités et positions respectives de Bruxelles Environnement - IBGE et celles reprises dans le message privé du membre du personnel lui-même.

Les comportements suivants sont interdits :

- ✘ utiliser des services permettant l'échange d'idées et discussions en temps réel (chat) ou différé (newsgroup), sauf si un tel accès est expressément autorisé par la Direction générale ;
- ✘ accéder à des sites payants, sans autorisation préalable de la Direction générale. En cas de transgression, le remboursement des sommes engagées sera demandé par Bruxelles Environnement - IBGE, par voie judiciaire, le cas échéant, et une récupération sur salaire sera mise en œuvre ;
- ✘ participer à la création d'un site ou utiliser le logo de Bruxelles Environnement - IBGE, sans autorisation expresse de la Direction générale ;
- ✘ accéder à des sites où il est porté atteinte à la dignité d'autrui, eu égard aux textes légaux et réglementaires, et notamment, sans que cette liste soit exhaustive :

  - 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, chapitre V, sanctionnant les atteintes portées à l'honneur ou à la considération des personnes (calomnie, diffamation, injures) …

  - dont le contenu est jugé illicite (publications interdites par la loi ou non légalement accessibles) ou préjudiciable à un tiers : - à caractère pornographique ;
    - sans son autorisation préalable.

En outre, l'utilisation des systèmes informatiques de Bruxelles Environnement - IBGE pour commettre des actes de criminalité informatique est interdite et pénalement réprimée.

**ARTICLE 7 : REGLES SPECIFIQUES A L'UTILISATION DU RESEAU INTERNE**

Le réseau informatique de Bruxelles Environnement – IBGE est réservé exclusivement à l'exercice de l'activité professionnelle, il ne peut donc contenir que des fichiers, base de données, programmes etc… nécessaires à l'accomplissement des missions de Bruxelles Environnement – IBGE.

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

Ces fichiers sont stockés à deux endroits particuliers:

1. Les groupes réseaux
2. Le répertoire MyDocuments de tous les pc de Bruxelles Environnement – IBGE (redirigé vers le réseau pour une plus grande sécurité des données et un backup)

Les fichiers personnels ne peuvent en aucun cas être stockés à ces endroits.

Si des fichiers personnels doivent être stockés sur le PC de manière temporaire ou à plus longue durée ils devront être stockés dans des répertoires créés à cet effet sur les disques locaux C:\ et/ou D:\ et ce dans les limites des capacités disques disponibles.
Dans tous les cas la confidentialité de ces documents ne peut être garantie que si l'utilisateur indique de manière claire que les documents placés sur le PC sont strictement personnels (utiliser un répertoire "personnel").
Il est à noter qu'aucun backup de ces fichiers personnels ne sera effectué. En cas de crash machine ces données seront perdues.

**ARTICLE 8 : GESTION DU RESEAU D'INFORMATION ET SURVEILLANCE PAR LES ADMINISTRATEURS SYSTEMES**

Mesures de prévention:

Les gestionnaires du réseau privilégient les mesures préventives qui visent à garantir la sécurité et l'intégrité des systèmes informatiques :

- L'accès au réseau informatique de Bruxelles Environnement – IBGE, depuis les sites extérieurs et depuis l'intérieur, est réservé aux utilisateurs dûment identifiés.

- Bruxelles Environnement – IBGE détermine, en fonction des besoins du service, quelles sont les ressources accessibles à chaque utilisateur, notamment au niveau des répertoires, des programmes informatiques et des bases de données.

- Les gestionnaires du réseau mettent en place de manière préventive les outils nécessaires à assurer la sécurité du système et empêcher le risque d'intrusion sous quelque forme que ce soit.
  Ainsi les gestionnaires du réseau en concertation avec le responsable du département informatique peuvent être amenés à
  ~ Bloquer l'accès aux sites internet dont le contenu est illégal, offensant ou inapproprié avec la mission de service public de l'institut. (voir ci-dessus) (ex : les sites à caractère pornographique)
  ~ 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…)[1].
  ~ Limiter la taille des fichiers attachés en fonction des ressources réseau disponibles (bande passante, espace de stockage…)

[1] Le département informatique a dû renforcer sans cesse les mesures de sécurité face à la prolifération des virus et tentatives d'intrusion de notre réseau (hacking, spam, phishing, etc…). Ainsi, outre un système de sécurité complexe et coûteux, certains types de fichiers attachés ont été désormais interdits (ex: les fichiers .exe)

~ Supprimer certains courriers électroniques ou fichiers attachés sans prendre connaissance de leur contenu lorsque les systèmes de détection informatiques ont reconnu une menace pour la sécurité (virus, SPAM, vers, cheval de troie, ouverture de porte réseau, envoi massif de mail…)

En cas de nouvelle mesure en application celle-ci fera l'objet d'une information préalable à l'ensemble du personnel.

Il ne pourra être dérogé à cette règle d'information qu'en cas de force majeure mettant en péril la sécurité des systèmes (ex: un site web ou un type de fichier faisant l'objet de publicité sur son caractère dangereux ou le fait de dissimuler un virus). Le blocage envisagé visera uniquement à la préservation du système informatique de Bruxelles environnement et sera à caractère temporaire. Tout autre type de blocage fera l'objet comme ci-dessus d'une publicité interne.

Si pour une raison de service, une des règles ci-dessus venait à poser problème, chaque utilisateur a la possibilité d'en avertir le helpdesk ICT afin de se voir proposer une solution satisfaisante dans un délai raisonnable.
**Comment faire ?**
**Ouvrir un Ticket via GLPI (voir intranet ou raccourci dans START)**
**Tél : 990**
Mail : helpdeskict@ibgebim.be

Le Département informatique exerce la gestion et l'analyse des flux d'informations entrants et sortants, pour des raisons liées à la sécurisation des systèmes informatiques et au bon fonctionnement du réseau de Bruxelles Environnement - IBGE.

Ces activités sont réalisées dans le respect de la vie privée, notamment des travailleurs sur le lieu de travail, ainsi que dans le respect des informations couvertes par le secret professionnel, et n'ont pas pour objet d'établir un lien individuel entre les adresses des sites consultés et une personne en particulier.

Elles concernent exclusivement des données de trafic et non des données à caractère personnel. La collecte est globale. Il s'agit de contrôler la durée de connexion par poste de travail, l'usage du courrier électronique (nombre et volume de courriers sortants), sans possibilité d'identifier le travailleur, ce contrôle étant inhérent à la gestion d'un système informatique.

Elles s'effectuent ponctuellement :

- ✓ en cas de problème du système informatique ou du réseau laissant supposer que le problème provient d'une utilisation inadéquate ou abusive de l'outil. Les administrateurs système peuvent examiner les caractéristiques des messages susceptibles d'être à l'origine du problème, sans prendre connaissance du contenu, en se basant sur des critères tels que la taille, le type, l'extension, la quantité de fichiers attachés.

- ✓ pour localiser et récupérer des informations professionnelles essentielles qu'il est impossible d'obtenir par d'autres moyens (force majeure, …)

Selon les moyens suivants et à la source de la connexion Internet :

- ✓ utilisation de logiciels qui identifient l'expédition de courriers en chaîne ;

- ✓ utilisation de logiciels qui isolent et/ou bloquent les courriels, fichiers, … interdits, et/ou bloquent le téléchargement de tels documents ;

- ✓ repérage des sites suspects ;

- ✓ scannage des messages à l'entrée pour déterminer la présence d'un virus éventuel ;

- ✓ destruction sans préavis des fichiers non autorisés et qui font l'objet d'une interdiction et répression pénale.

Celles-ci ne sont pas nominatives, elles mentionnent le moment de la connexion, sa durée, les volumes échangés et le cas échéant, les adresses des sites visités.

Il y a lieu de préciser la permanence ou non du contrôle.

Il y a lieu de mentionner le mode de conservation des données, son lieu et sa durée.

Chaque personne a un droit d'accès de rectification des données le concernant.

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

Un responsable du traitement est désigné et représente Bruxelles Environnement - IBGE auprès de la Commission de la protection de la vie privée. Une déclaration par le maître de fichier est adressée à la dite Commission.

**ARTICLE 9: COMMUNICATION**

L'information est individuelle et collective.

Chaque personne est informée que le PC sur lequel elle travaille peut être contrôlé et que des statistiques globales sont collectées par la cellule informatique.

Les consignes d'utilisation sont mentionnées sur écran à l'allumage et/ou lors de l'activation de certains programmes.

Les représentants du personnel sont préalablement avertis de la mise en œuvre de chaque intervention.

Les consignes d'utilisation sont mentionnées sur écran à l'allumage et/ou lors de l'activation de certains programmes.

Si nécessaire des codes de bonnes pratiques relatifs à des outils particuliers seront édités et mis à disposition du personnel via l'intranet afin de les guider et les informer sur les outils disponibles et la façon de les utiliser.

Contacter le helpdesk

**Comment faire ?**
**Ouvrir un Ticket via GLPI (voir intranet ou raccourci dans START)**
**Tél : 990**
Mail : helpdeskict@ibgebim.be

**ARTICLE 10 : CONTROLE**

Le contrôle est réalisé selon les principes de finalité, de proportionnalité et de transparence.

- Les finalités (ou données) sont déterminées, explicites et légitimes. Elles sont énumérées de manière exhaustive :

  * La prévention de faits illicites, contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui : propos diffamatoire, 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, …

  * La sécurité et/ou le fonctionnement technique des systèmes informatiques en réseau : actes de piratage informatique notamment.

* Le respect de bonne foi des règles et principes d'utilisation des technologies.

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

Un contrôle non individuel est réalisé, en cas de non respect du principe de l'exécution de bonne foi ou d'anomalie.

Une individualisation des données peut être requise en cas de récurrence et si l'anomalie nécessite une identification du responsable et eu égard aux deux premières finalités mentionnées.
Le traitement est limité par rapport au contenu des données, de manière à pouvoir identifier une personne.

Un contrôle individuel, ponctuel et dûment justifié peut être effectué, dans les conditions suivantes :

- Lorsque des éléments probants démontrent une utilisation contraire à la présente instruction, une décision motivée de mise sous surveillance est envisagée à l'égard de l'agent concerné.

~ Il faut des indices concordants laissant suspecter une utilisation répétée et incompatible des moyens de télécommunications.

- La mesure de surveillance est communiquée préalablement à sa mise en œuvre à l'intéressé et une audition de l'intéressé en présence d'un représentant du personnel, s'il le souhaite, a lieu dans les 10 jours.

~ L'information faite à l'agent concerné porte sur les prérogatives de la Direction en la matière, ainsi que les droits et obligations du personnel chargé du traitement, la nature du contrôle, les finalités et les modalités de celui-ci, ainsi que sur les sanctions susceptibles d'être prises.

Le département informatique n'est pas compétent pour prendre une telle décision. Seule la Direction générale y est habilitée. Elle donne ensuite l'autorisation écrite au département informatique de procéder à la surveillance.

~ Les données recueillies lors du contrôle portent sur le trafic des communications, à l'exception de leur contenu.

~ Le contrôle est temporaire et se limite aux communications sortantes.

~ Son but légitime repose sur la protection des droits de l'homme et libertés fondamentales, sur la sécurité publique et la prévention ou répression des infractions pénales.

Dans le cadre de l'utilisation d'intranet (petites annonces, forums, plus précisément), un contrôle sera exercé par le service communication en vue de respecter les règles mentionnées à l'article 5

**ARTICLE 11 : SANCTIONS**

Le non-respect de la présente instruction est susceptible de donner lieu à l'une des sanctions suivantes, en fonction de la gravité du manquement en cause :

- Avertissement écrit reprenant le fait reproché.

- Retrait de l'utilisation du courriel ou de l'accès à Internet, soit temporairement, soit définitivement ;

- Application proportionnelle des sanctions prévues par la législation applicable à la relation qui unit le membre du personnel à l'organisme ;

- Mise en cause devant les juridictions compétentes de la responsabilité civile $^{et}/_{ou}$ pénale de l'intéressé.

L'auteur de comportements réprimés et érigés en infractions pénales visés aux articles 4 et 5 de la présente instruction s'expose au licenciement pour faute grave, à une sanction disciplinaire ou à toute autre mesure, en fonction de la gravité de son comportement.

**ARTICLE 12 : EVALUATION**

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.

**ARTICLE 13 : TRANSPARENCE ET PUBLICITE**

Conformément aux termes de la loi du 19 décembre 1974, une concertation relative à la présente instruction a eu lieu, en date du JJ.MM.AAAA

La présente instruction a fait l'objet d'une publicité par voie d'avis au personnel, à partir du JJ MMMM AAAA.

# BIJLAGE 11 : CHARTER VOOR HET GEBRUIK VAN DE INFORMATICATOOLS DIE TER BESCHIKKING WORDEN GESTELD VAN HET PERSONEEL VAN LEEFMILIEU BRUSSEL – BIM

## VOORWOORD

Deze richtlijn werd opgesteld op basis van een aantal bepalingen met de bedoeling de beschikbare communicatiemiddelen bij Leefmilieu Brussel – BIM en met name de toegang tot het internet en het gebruik van e-mail overeenkomstig de wet, de mensenrechten en de fundamentele vrijheden te gebruiken:

- het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en met name artikel 8;
- richtlijn 95/46/EG van het Europees Parlement en van de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens;
- de Grondwet en met name artikel 22;
- de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van de persoonsgegevens gewijzigd door de wet van 11 december 1998 en met name artikel 16 § 3 waarin verplicht wordt de veiligheid van de gegevens uit de persoonlijke levenssfeer die ingezameld en bewaard werden door de houder van het bestand te waarborgen door elke technische en organisatorische maatregel die vereist is om de beheerde bestanden te beschermen;
- de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven die de kennisname door een derde van per telecommunicatie verzonden gegevens verbiedt en met name artikel 109 ter D;
- de strafwet en met name artikel 314 bis dat het beluisteren, de kennisneming en de registratie van mededelingen of mededelingen per telecommunicatie uit de persoonlijke levenssfeer zonder toestemming van alle betrokkenen bestraft;
- de aansprakelijkheid als houder van een persoonsregistratie;
- het advies nr. 10/2000 van 3 april 2000 van de Commissie voor de bescherming van de persoonlijke levenssfeer.

Het ter beschikking stellen van de communicatiemiddelen door Leefmilieu Brussel – BIM aan het personeel van de Instelling wordt door de volgende doelstellingen ondersteund :

- de interne en externe communicatie vergemakkelijken ;
- een doeltreffend en gepast werkmiddel bieden in het kader van de nieuwe technologieën;
- het aanleren, het gebruik en de evolutie van deze nieuwe technologieën aanmoedigen opdat de geleverde werkkwaliteit en de vaardigheden van het personeel op dit vlak verbeteren.

**ARTIKEL 1 : TOEPASSINGSDOMEIN**

De voorliggende richtlijn heeft betrekking op het volledige personeel van Leefmilieu Brussel – BIM, of het nu gaat over statutaire, administratieve of pedagogische contractuele medewerkers of anderen, in welke functie dan ook, in de mate dat er een verband van ondergeschiktheid tussen de medewerker en de Instelling bestaat.

**ARTIKEL 2 : EIGENDOMSRECHT**

Het materiaal dat door Leefmilieu Brussel – BIM op de werkplek, zelfs occasioneel, ter beschikking van het personeel wordt gesteld, behoort Leefmilieu Brussel – BIM toe.

**ARTICLE 3 : GEBRUIKS- EN TOEGANGSMODALITEITEN**

Iedereen die over een toegang tot de informatiesystemen beschikt, gebruikt deze voor beroepsdoeleinden, m.a.w. voor de uitoefening van zijn functie.

Hij / zij is verantwoordelijk voor het gebruik dat hij / zij maakt van de informatiesystemen en gebruikt ze als een goede huisvader.

Bij het gebruik en het zich toegang verschaffen moet men bovendien rekening houden met de vereisten voor de veiligheid en de goede werking van de systemen met het doel ze te beschermen tegen risico's zoals virusinfecties of binnendringing.

Daarom stelt Leefmilieu Brussel – BIM de noodzakelijke middelen ter beschikking om de toegangen tot de vermelde systemen te beveiligen.

Het is verboden om zonder toelating in te loggen op de account (e-mail of netwerk) van een collega, of die nu aanwezig is of niet, en zijn account te gebruiken om niet-getolereerde boodschappen te versturen.

De toegang van gebruikers tot bewaarde informatie en documenten op de informaticasystemen moet beperkt worden tot de eigen documenten (MyDocuments) en de openbare of gedeelde documenten. Het is in het bijzonder verboden om kennis te nemen van informatie die bij andere gebruikers zit, zelfs als ze die niet uitdrukkelijk beschermd zouden hebben. Deze regel is eveneens van toepassing op privégesprekken van het e-mailtype die niet rechtstreeks of in kopie aan de gebruiker geadresseerd zijn.

Aanbevelingen

- Elke gebruiker moet elke poging tot inbreuk in zijn account en in het algemeen elke vastgestelde onregelmatigheid melden.

- Voor elke software-installatie moet de gebruiker een aanvraag via de helpdesk doen.

  **Hoe ?**
  **Open een ticket met VBIP (zie intranet or snelkoppeling in START)**
  **Tel. : 990**
  E-mail : helpdeskict@ibgebim.be

- Elke gebruiker moet er zich toe verbinden om geen toegang tot de systemen of tot de netwerken via het materieel dat hij / zij gebruikt aan niet-geautoriseerde gebruikers te verschaffen.
- De gebruiker let erop dat hij / zij bij het verlaten van de werkpost deze vergrendelt (Ctrl+alt+del) en hem niet open voor gebruik laat staan.
-

**ARTIKEL 4 : SPECIFIEKE REGELS VOOR HET GEBRUIK VAN E-MAIL**

- E-mail moet oordeelkundig gebruikt worden.

- Door de wet verboden boodschappen die eventueel bij een personeelslid van de Instelling kunnen aankomen, moeten onmiddellijk gewist worden. Het personeelslid is niet verantwoordelijk voor de inhoud van de boodschappen die hij / zij ontvangt, maar kan als verantwoordelijk voor het gebruik of het doorzenden van de ontvangen boodschappen beschouwd worden. Als de afzender zulke e-mail hardnekkig blijft doorsturen moet het personeelslid hem / haar vragen om onmiddellijk de verzendingen stop te zetten, voor zover de afzender identificeerbaar is en men zulke stappen kan ondernemen.

Het e-mailgebruik voor privédoeleinden wordt onder de volgende voorwaarden toegestaan :

- ✓ het goede beheer van Leefmilieu Brussel - BIM wordt niet belemmerd, men mag e-mail namelijk niet gebruiken ten nadele van activiteiten die de Instelling uitoefent ;

- ✓ het vormt geen inbreuk op de voorliggende richtlijn en gaat niet in tegen de wettelijke bepalingen ;

- ✓ Leefmilieu Brussel – BIM kan niet aansprakelijk gesteld worden ;

- ✓ het imago van de instelling wordt niet geschaad en men roept geen verwarring in de geest van derden op wat betreft de respectieve identiteit en positie van Leefmilieu Brussel – BIM en die vermeld in de boodschap van het personeelslid zelf. In dit opzicht is het belangrijk om elke aanwijzing die erop zou wijzen dat de boodschap in het kader van de uitoefening van zijn functie opgesteld is uit te sluiten.

Deze gedragingen zijn verboden :

- ✘ uitnodigen tot of deelnemen aan een kettingbrief zonder sociaal nut;

- ✘ vertrouwelijke en / of persoonlijke gegevens aangaande de Instelling, het personeel, de stagiaires of de partners te verspreiden, behoudens de uitdrukkelijke toelating van de rechthebbenden of door de wet bepaalde uitzonderingen ;

- ✘ de reproductie, verspreiding, het mededelen, onder welke vorm ook, van informatie die de waardigheid van de andere kan aantasten. Dit in navolging van een aantal wet- en reglementaire teksten, met name (zonder dat deze lijst exhaustief is):
  de wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden, de wet van 23 maart 1995 tot bestraffing van het ontkennen, onderschatten, rechtvaardigen of goedkeuren van de genocide die tijdens de Tweede Wereldoorlog door het Duitse nationaal-socialistisch regime is gepleegd, artikelen 383 en volgende van het strafwetboek met betrekking tot de openbare zedenschennis en met name 383 bis dat de verspreiding of het bezit van documenten van pornografische aard met betrekking tot minderjarigen bestraft; artikelen 443 en volgende van het strafwetboek, hoofdstuk V, die aantasting van de eer of de goede naam van personen (laster, smaad, beledigingen, …) bestraft.

  - waarvan de inhoud niet wettelijk is (door de wet verboden of niet wettelijk toegankelijke publicaties) of die een derde schade kan toebrengen : - van pornografische aard ;
    - zonder voorafgaande toestemming;

  - zich onrechtmatig de identiteit of de titel van een andere toe-eigenen door zonder medeweten en / of in zijn / haar naam een e-mail te versturen ;

  - door het auteursrecht, het recht van producenten van databanken, … beschermde gegevens te verspreiden, behoudens toelating van de rechthebbende ;

  - op illegale wijze verkregen informatie te verspreiden ;

  - e-mail in het kader van een beroepsactiviteit buiten het werkverband te gebruiken.

Het is ten slotte aangewezen om de openbare orde, de goede zeden, het portretrecht, de persoonlijke levenssfeer, het briefgeheim na te leven.

Uit respect voor de vertrouwelijkheid van de mededelingen is het verboden om toegang proberen te krijgen tot elektronische boodschappen van iemand anders of ze te lezen zonder voorafgaand akkoord van de belanghebbende (correct gegeven delegering).

Aanbevelingen

- Elke gebruiker raadpleegt regelmatig zijn inkomende e-mails en geeft gevolg aan de boodschappen die om een antwoord vragen.

- Elke gebruiker ziet erop toe dat hij / zij geleidelijk de behandelde boodschappen wist met het doel het informaticasysteem niet te overbelasten. Indien nodig ziet hij / zij toe op het archiveren of klasseren van sommige boodschappen. In dit kader worden sommige tools nu en in de toekomst ter beschikking gesteld. De noodzakelijke opleidingen worden eveneens georganiseerd.

- Elke gebruiker ziet erop toe een kopie van de ontvangen boodschappen te sturen naar de personen die hierover op de hoogte gesteld moeten worden, maar vermijdt ook overbodige verzendingen.

- Ingeval van verlengde afwezigheid wordt aanbevolen om de correspondenten op de hoogte te brengen door een automatisch antwoord voor afwezigheid met vermelding van de duur en de naam alsook de gegevens van de persoon tot wie men zich dient te wenden ingeval van nood.

- Elke gebruiker wordt eraan gehouden uiterst voorzichtig met de boodschappen die hij / zij verzendt om te gaan. Ingeval van deelname aan een forum op persoonlijke gronden moet hij / zij aangeven dat de boodschap enkel en alleen zijn / haar persoonlijke opinie weergeeft.

- Bij inschrijving ter persoonlijke titel op fora of sociale netwerken is het gebruik van het professionele e-mailadres verboden. In dit geval wordt er aangeraden het privé-e-mailadres te gebruiken.

**ARTIKEL 5 : SPECIFIEKE REGELS VOOR HET INTRANETGEBRUIK**

Deze gedragingen zijn verboden :

✘ de reproductie, verspreiding, het mededelen, onder welke vorm ook, van informatie die de waardigheid van de ander kan aantasten. Dit in navolging van een aantal wet- en reglementaire teksten, met name (zonder dat deze lijst exhaustief is):

de wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden, de wet van 23 maart 1995 tot bestraffing van het ontkennen, onderschatten, rechtvaardigen of goedkeuren van de genocide die tijdens de tweede wereldoorlog door het Duitse nationaal-socialistisch regime is gepleegd, artikels 383 en volgende van het strafwetboek met betrekking tot de openbare zedenschennis en met name 383 bis dat de verspreiding of het bezit van documenten van pornografische aard met betrekking tot minderjarigen bestraft; artikels 443 en volgende van het strafwetboek, hoofdstuk V, die aanrandingen van de eer of de goede naam van personen (laster, smaad, beledigingen, …) bestraft.

- informatie waarvan de inhoud niet wettelijk is (door de wet verboden of niet wettelijk toegankelijke publicaties) of die schade aan een derde kan toebrengen : - van pornografische aard ;
  - zonder voorafgaande toestemming;

- zich onrechtmatig de identiteit of de titel van een andere toe-eigenen ;

- het auteursrecht, het recht van producenten van databanken, … beschermde gegevens verspreiden, behoudens toelating van de rechthebbende ;

- op illegale wijze verkregen informatie verspreiden.

Ten slotte is het aangewezen om de openbare orde, de goede zeden, het portretrecht, de persoonlijke levenssfeer, het briefgeheim na te leven.

**ARTIKEL 6 : SPECIFIEKE REGELS VOOR HET SURFEN OP INTERNET**

Bij het surfen op het internet moet iedereen bijzonder aandachtig zijn voor websites die pas toegankelijk worden als de surfer zich identificeert. In dit geval handelt hij / zij uit eigen naam.

Voor het personeel dat over een internettoegang beschikt, wordt het internetgebruik voor privédoeleinden onder de volgende voorwaarden toegestaan :

- ✓ het wordt gebruikt vanuit het oogpunt bij te leren en zich persoonlijk te ontwikkelen ;
- ✓ het gebruik is occasioneel ;
- ✓ het gebruik belemmert het goede beheer van Leefmilieu Brussel – BIM niet, het gebeurt nl. niet ten nadele van activiteiten die de Instelling uitoefent ;
- ✓ het gebruik mag geen inbreuk vormen op de voorliggende richtlijn en niet ingaan tegen de wettelijke bepalingen ;
- ✓ bij het gebruik kan men Leefmilieu Brussel – BIM niet aansprakelijk stellen ;
- ✓ het imago van de Instelling wordt niet geschaad en men roept geen verwarring in de geest van derden op wat betreft de respectieve identiteit en positie van Leefmilieu Brussel – BIM en die vermeld in de boodschap van het personeelslid zelf.

Deze gedragingen zijn verboden :

- ✘ het gebruik van diensten waarmee men ogenblikkelijk (chatten) of met tussentijd (newsgroup) ideeën uitwisselen en discussies voeren kan, behalve als zulk een toegang uitdrukkelijk door de Algemene directie toegestaan wordt ;
- ✘ zich toegang tot betaalsites verschaffen zonder voorafgaande toelating van de Algemene directie. Ingeval van overtreding wordt de terugbetaling van de toegezegde bedragen door Leefmilieu Brussel – BIM desgevallend langs juridische weg gevraagd en er wordt een inhouding op het loon toegepast ;
- ✘ deelnemen aan het maken van een website en het logo van Leefmilieu Brussel - BIM gebruiken zonder uitdrukkelijke toestemming van de Algemene directie ;
- ✘ zich toegang verschaffen tot websites waarin de waardigheid van de andere wordt aangetast. Dit in navolging van een aantal wet- en reglementaire teksten, met name (zonder dat deze lijst exhaustief is):

  de wet van 30 juli 1981 tot bestraffing van bepaalde door racisme of xenofobie ingegeven daden, de wet van 23 maart 1995 tot bestraffing van het ontkennen, onderschatten, rechtvaardigen of goedkeuren van de genocide die tijdens de tweede wereldoorlog door het Duitse nationaal-socialistisch regime is gepleegd, artikels 383 en volgende van het strafwetboek met betrekking tot openbare de zedenschennis en met name 383 bis dat de verspreiding of het bezit van documenten van pornografische aard met betrekking tot minderjarigen bestraft; artikels 443 en volgende van het strafwetboek, hoofdstuk V, die aanrandingen van de eer of de goede naam van personen (laster, smaad, beledigingen, …) bestraft.

  - informatie waarvan de inhoud niet wettelijk is (door de wet verboden of niet wettelijk toegankelijke publicaties) of die schade aan een derde kan toebrengen : - van pornografische aard ;
    - zonder voorafgaande toestemming;
  - zich onrechtmatig de identiteit of de titel van een ander toe-eigenen ;

- het auteursrecht, het recht van producenten van databanken, … beschermde gegevens verspreiden, behoudens toelating van de rechthebbende ;

- op illegale wijze verkregen informatie verspreiden.

Het gebruik van de informaticasystemen van Leefmilieu Brussel - BIM om daden van computercriminaliteit te stellen wordt daarenboven verboden en strafrechtelijk beteugeld.

**ARTIKEL 7 : SPECIFIEKE REGELS VOOR HET GEBRUIK VAN HET INTERN NETWERK**

Het informaticanetwerk van Leefmilieu Brussel – BIM wordt uitsluitend voor de uitoefening van beroepsactiviteiten voorbehouden. Het mag dus enkel bestanden, gegevensbanken, programma's, enz. … die noodzakelijk zijn om de opdrachten van Leefmilieu Brussel – BIM ten uitvoer te brengen bevatten.

De bestanden die er opgeslagen worden, beschouwt men als beroepsmatige bestanden.

Deze bestanden worden op twee bepaalde plekken opgeslagen:
1. de netwerkgroepen
2. de map MyDocuments van alle pc's van Leefmilieu Brussel – BIM (voor meer veiligheid van de gegevens en een back-up terug naar het netwerk afgeleid).

Persoonlijke bestanden kunnen in geen enkel geval op deze plekken opgeslagen worden.

Als persoonlijke bestanden op tijdelijke wijze of op langere duur op de PC opgeslagen moeten worden, moeten ze in voor dit doel aangemaakte mapjes op de lokale C:\- en of D:\-schijf aangemaakt worden en dit binnen de grenzen van de beschikbare diskcapaciteit.
In al deze gevallen kan de vertrouwelijkheid van deze documenten slechts gegarandeerd worden als de gebruiker op duidelijke wijze aanduidt dat de op de PC geplaatste documenten strikt persoonlijk zijn (een mapje "Persoonlijk" gebruiken).
Er dient opgemerkt te worden dat geen enkele back-up van deze persoonlijke bestanden wordt uitgevoerd. Wanneer de computer crasht, zijn deze gegevens verloren.

**ARTIKEL 8 : BEHEER VAN HET INFORMATIENETWERK EN TOEZICHT DOOR DE SYTEEMBEHEERDERS**

Preventieve maatregelen

De netwerkbeheerders maken bij voorkeur gebruik van de preventieve maatregelen met het oog op het veiligstellen van de veiligheid en de integriteit van de informaticasystemen:

- de toegang tot het informaticanetwerk van Leefmilieu Brussel – BIM vanaf externe websites en van binnenuit wordt voor correct geïdentificeerde gebruikers voorbehouden.
- Leefmilieu Brussel - BIM bepaalt in functie van de noden van de dienst welke middelen voor elke gebruiker toegankelijk zijn, met name aangaande de mappen, de informaticaprogramma's en de gegevensbanken.

- de netwerkbeheerders voorzien op preventieve wijze in de noodzakelijke tools om de veiligheid van het systeem te garanderen en het risico op binnendringen, in welke vorm dan ook, te verhinderen.
  Zo is het mogelijk dat de netwerkbeheerders in overleg met het hoofd van het informaticadepartement ertoe komen om :
  ~ de toegang te blokkeren tot websites met illegale, beledigende of niet met de opdracht van overheidsdienst van het Instituut strokende inhoud (zie hierboven) (bijv. : websites van pornografische aard);
  ~ het downloaden te verbieden van sommige types van door hun formaat geïdentificeerde bestanden omdat ze zonder reden die in verband met de activiteit staat een beroep op de netwerkmiddelen doen of omdat ze een eventueel gevaar voor de veiligheid vormen of omdat ze

de informaticasystemen kunnen beschadigen (bijvoorbeeld: de bestanden van uitvoerbare bestanden …)[1];

~ de grootte van de bijgevoegde bestanden in functie van de beschikbare netwerkmiddelen (bandbreedte, opslagruimte, …) te beperken;

~ sommige e-mails of bijgevoegde bestanden te verwijderen zonder van hun inhoud kennis te nemen wanneer de informaticadetectiesystemen een bedreiging voor de veiligheid opgespoord hebben (virus, SPAM, wormen, Trojaans paard, opening van de netwerkpoort, massale e-mailverzending, …).

Bij toepassing van een nieuwe maatregel wordt het volledige personeel hierover voorafgaandelijk geïnformeerd.

Op deze regel van informatieverstrekking mag slechts afgeweken worden ingeval van overmacht, wanneer de veiligheid van de systemen in het gedrang komt (bijv.: een website of een type van bestand waarvoor men reclame maakt over de gevaarlijke aard ervan of het feit dat het een virus verbergt). Het blokkeren dat hier wordt bedoeld heeft als enige doel het informaticasysteem van Leefmilieu Brussel te vrijwaren en is van tijdelijke aard. Elk ander type van blokkeren wordt zoals hierboven intern onder de aandacht gebracht.

Stelt een van de regels hierboven omwille van een dienstreden een probleem, dan heeft elke gebruiker de mogelijkheid om de ICT-helpdesk ervan op de hoogte te stellen zodat deze op redelijke termijn een bevredigende oplossing voorstellen kan.
**Hoe ?**
**Open een ticket met VBIP (zie intranet or snelkoppeling in START)**
**Tel. : 990**
E-mail : helpdeskict@ibgebim.be

Omwille van redenen in verband met de beveiliging van de informaticasystemen en het goede functioneren van het netwerk van Leefmilieu Brussel – BIM voert het informaticadepartement het beheer en de analyse van de binnenkomende en uitgaande informatiestromen uit.

Deze activiteiten worden uitgevoerd met respect voor de persoonlijke levenssfeer, met name van de werknemers op de werkplaats, alsook met respect voor de informatie die door het beroepsgeheim beschermd wordt en hebben niet de bedoeling een individueel verband tussen de adressen van de geraadpleegde bestanden en een persoon in het bijzonder te bewerkstelligen.

Deze activiteiten betreffen uitsluitend uitgewisselde gegevens en niet gegevens van persoonlijke aard. De inzameling is globaal. Het gaat erom de verbindingsduur per werkpost, het gebruik van e-mail (aantal en volume van uitgaande e-mails) te controleren zonder mogelijkheid om de werknemer te identificeren. Deze controle is onlosmakelijk verbonden met het beheer van een informaticasysteem.

Deze activiteiten gaan door op gezette tijdstippen :

✓ bij een probleem van het informaticasysteem of van het netwerk dat laat vermoeden dat het probleem afkomstig is van een oneigenlijk of overmatig gebruik van de tool kunnen de systeembeheerders de eigenschappen van de boodschappen die mogelijk aan de oorzaak van dit probleem liggen, onderzoeken zonder kennis van de inhoud te nemen en zich hierbij baseren op criteria zoals de grootte, het type, de extensie, de hoeveelheid bijgevoegde bestanden.

✓ om essentiële beroepsmatige informatie die onmogelijk op andere wijze kan worden verkregen op te sporen en terug te winnen (overmacht, …).

Volgens de volgende middelen :

✓ gebruik van de softwareprogramma's die het versturen van kettingmails identificeren ;

[1] Het informaticadepartement heeft onophoudelijk de veiligheidsmaatregelen tegenover de verspreiding van virussen en pogingen om in ons systeem binnen te dringen (hacking, spam, phishing, enz. …) moeten aanscherpen. Zo werden, bovenop een complex en kostelijk beveiligingssysteem sommige types van bijgevoegde bestanden ondertussen verboden (bijv.:.exe-bestanden).

- ✓ gebruik van softwareprogramma's die verboden e-mails, bestanden, … isoleren en / of blokkeren en / of het downloaden van zulke documenten blokkeren ;
- ✓ verdachte websites opsporen ;
- ✓ scannen van binnenkomende boodschappen om de aanwezigheid van een eventueel virus te bepalen ;
- ✓ vernietiging zonder waarschuwing vooraf van niet toegestane bestanden waarop een verbod en een bestraffing rust.

Deze activiteiten vermelden geen naam, ze vermelden het ogenblik van de verbinding, de duur, de uitgewisselde volumes en desgevallend de adressen van de bezochte websites.

Het is aangewezen om duidelijk aan te geven of de controle al dan niet permanent is.

Het is aangewezen om de wijze, de plaats en de duur van het bewaren van de gegevens te vermelden.

Elke persoon heeft rectificatietoegangsrecht voor de hem betreffende gegevens.

De vertrouwelijkheid en de veiligheid van de gegevensverwerking zijn gegarandeerd.

Er wordt een verantwoordelijke voor de verwerking aangesteld die Leefmilieu Brussel – BIM bij de Commissie voor de bescherming van de persoonlijke levenssfeer vertegenwoordigt. De houder van de persoonsregistratie verstuurt een verklaring naar de voornoemde Commissie.

**ARTIKEL 9: COMMUNICATIE**

De informatieverstrekking gebeurt op individuele basis en in groep.

Iedereen wordt op de hoogte gebracht dat de PC waarop hij / zij werkt gecontroleerd kan worden en dat de informaticacel globale statistieken inzamelt.

De gebruiksaanwijzingen worden op het scherm vermeld bij het aanschakelen en / of bij het openen van bepaalde programma's.

De personeelsvertegenwoordigers worden op de hoogte gebracht van interventies die zullen plaatsvinden.

De gebruiksaanwijzingen worden op het scherm vermeld bij het aanschakelen en / of bij het openen van bepaalde programma's.

Indien nodig worden er richtlijnen voor goede praktijken met betrekking tot bepaalde tools uitgevaardigd en via intranet ter beschikking van het personeel gesteld zodat het begeleiding en informatie heeft over de beschikbare tools en het gebruik ervan.

De helpdesk contacteren.

**Hoe ?**

**Open een ticket met VBIP (zie intranet or snelkoppeling in START)**
**Tel. : 990**
E-mail : helpdeskict@ibgebim.be

**ARTIKEL 10 : CONTROLE**

De controle wordt gerealiseerd volgens de principes van finaliteit, proportionaliteit en transparantie.

- De doelstellingen (of gegevens) zijn vastgesteld, uitdrukkelijk en gegrond. Ze worden uitvoerig opgesomd:

* de preventie van onwettige feiten, ingaand tegen de goede zeden of die mogelijk de waardigheid van de andere aantast : beledigend voorstel, gegevens van pornografische of pedofiele aard, feiten die aanzetten tot discriminatie, tot segregatie, tot haat of tot geweld volgens ras, huidskleur, afstamming, religie, nationale of etnische afkomst, verspreiding van bestanden of vertrouwelijke gegevens met betrekking tot bijvoorbeeld het personeelsbeheer of geneeskundige informatie, ... ;

* de veiligheid en / of het technische functioneren van de informaticasystemen op het netwerk : met name daden van informaticapiraterij;

* het oprechte naleven van de regels en de gebruiksprincipes van de technologieën.

- De ingezamelde gegevens moeten ten aanzien van de vastgelegde doelstellingen aangepast, relevant en niet erg groot in aantal zijn.

Er wordt een niet-individuele controle uitgevoerd bij het niet naleven van het principe van uitvoering te goeder trouw of bij onregelmatigheid.

Een individualisering van de gegevens kan vereist zijn bij veelvuldig voorkomen en als de onregelmatigheid vraagt om een identificatie van de verantwoordelijke en rekening houdend met de twee eerste vermelde doelstellingen.
De verwerking wordt met betrekking tot de inhoud van de gegevens beperkt zodat een persoon geïdentificeerd kan worden.

Een individuele behoorlijk gerechtvaardigde controle op gezette tijdstippen kan onder de volgende voorwaarden uitgevoerd worden :

- wanneer afdoende elementen een gebruik dat ingaat tegen de voorliggende richtlijn aantonen, overweegt men een gemotiveerde beslissing om de betrokken medewerker onder toezicht te plaatsen;

~ er zijn samenhangende tekenen nodig die een herhaaldelijk en oneigenlijk gebruik van de telecommunicatiemiddelen doen vermoeden;

- de toezichtsmaatregel wordt voor het ingaan ervan aan de betrokkene meegedeeld. Binnen een termijn van 10 dagen vindt er een hoorzitting met de betrokkene in aanwezigheid van een personeelsvertegenwoordiger plaats, indien hij / zij dit wenst;

~ de betrokken medewerker wordt ingelicht over de voorrechten ter zake van de Directie alsook over de rechten en plichten van het personeel belast met de verwerking, de aard van de controle, de doelstellingen en de modaliteiten ervan alsook over de mogelijk te nemen sancties.

Het informaticadepartement is niet bevoegd om zulk een beslissing te nemen. Alleen de Algemene directie is er bevoegd voor verklaard. Ze geeft vervolgens schriftelijke toestemming aan het informaticadepartement om over te gaan tot het toezicht.

~ De bij de controle ingezamelde gegevens gaan over het communicatieverkeer, met uitzondering van de inhoud.

~ De controle is tijdelijk en beperkt tot de uitgaande mededelingen / gesprekken.

~ Het gegronde doel rust op de bescherming van de mensenrechten en de fundamentele vrijheden, op de openbare veiligheid en de preventie of beteugeling van de strafbare feiten.

In het kader van het intranetgebruik (meer bepaald kleine aankondigingen, fora) wordt er een controle door het communicatiedepartement uitgevoerd met het oog op de naleving van de regels vermeld onder artikel 5.

**ARTIKEL 11 : SANCTIES**

Het niet naleven van de voorliggende richtlijn kan aanleiding geven tot een van de volgende sancties, in functie van de ernst van het verzuim in kwestie :

- schriftelijke waarschuwing met melding van het aangewreven feit;
- inhouden van het e-mailgebruik of van de internettoegang, ofwel tijdelijk, ofwel definitief;
- evenredige toepassing van de sancties waarin voorzien wordt door de wetgeving van toepassing op de relatie die het personeelslid met de instelling verbindt ;
- de betrokkene in geding oproepen voor de voor burgerlijke en / of strafrechtelijke aansprakelijkheid bevoegde rechtbanken.

De dader van beteugelde gedragingen die op strafbare feiten neerkomen zoals bedoeld in artikel 4 en 5 van de voorliggende richtlijn loopt kans op een oneervol ontslag, op een tuchtsanctie of, in functie van de ernst van zijn gedrag, op elke andere maatregel.

**ARTIKEL 12 : EVALUATIE**

De geïnstalleerde controlesystemen worden regelmatig geëvalueerd door het Basisoverlegcomité, met name in verband met de revisie in functie van de technologische ontwikkelingen.

**ARTIKEL 13 : TRANSPARANTIE EN BEKENDMAKING**

Overeenkomstig de formulering van de wet van 19 december 1974 vindt een overleg met betrekking tot de voorliggende richtlijn plaats op DD.MM.JJJJ.

De voorliggende richtlijn werd kenbaar gemaakt door middel van een personeelsmededeling vanaf DD.MM. JJJJ.