ICT-POLICY

Richtlijnen ICT-middelen

Laatste wijziging: xx.xx.2020~~23.04.2018~~

HOOFDSTUK I.
ONDERWERP EN SCOPE.

Inleiding

Deze policy heeft als doel:

- het personeel te informeren over het gebruik van de ter beschikking gestelde ICT-middelen, en hen aan te sporen hier ten volle gebruik van te maken;
- de integriteit van het informaticasysteem van de Stad te garanderen;
- de gegevens die eigendom van de Stad zijn of betrekking hebben tot het privéleven van de personeelsleden of van burgers te beveiligen, en hun privacy te beschermen, in overeenstemming met de Privacywet.

Personeelsleden hebben in de regelmaat een eigen e-mailadres, toegang tot het internet en tot telefonie en elektronische communicatie, vanop hun vaste werkplek of eventueel mobiel. Dit document vertegenwoordigt het standpunt van de Stad betreffende het gebruik van het internet en ICT-middelen van haar personeelsleden alsook het monitoren van dit gebruik met respect voor de privacy. Overtreding van onderhavige richtlijnen kunnen aanleiding geven tot disciplinaire sancties.

Artikel 1.- De onderstaande begrippen welke meermaals gebruikt worden in deze policy zijn als volgt gedefinieerd:

Het personeelslid	Ieder die werknemer is van de Stad, welk juridisch verband er ook met de werkgever is (statutair of personeelslid met een arbeidsovereenkomst, kabinetsleden, stagiaire, aan de Stad gedetacheerden…). Niet inbegrepen is het onderwijzend personeel van het Publiek Onderwijs van de Stad.
De werkgever	De Stad en haar vertegenwoordigers aan wie het personeelslid verbonden is via een arbeidsovereenkomst of een statuut.
De policy	Het onderhavige document en al haar richtlijnen.
ICT-middelen	Een ruim begrip dat slaat op al wat het personeelslid gebruikt om verbinding te maken met het Internet of het netwerk, of om te communiceren, zij het materieel of digitaal, elektronisch of telefonisch, en in het bijzonder desktop computers, laptops, printers, vaste telefoons en mobile devices (tablets, smartphones, PDA's, …).
Het gegeven	Al wat opgeslagen en geklasseerd kan worden, op papier of digitaal, in letters en cijfers of met beeld of geluid.
Vertrouwelijke gegevens	Vertrouwelijke gegevens zijn gegevens die afhankelijk van de situatie - enkel voor intern gebruik bedoeld zijn, - enkel benaderd kunnen worden door een aantal gemachtigden, - of die beschermd zijn door de privacywet.
Privacywet	De Wet van 8 december 1992 voor de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.
Het bestand	Verzameling geordende (computer) gegevens, bv. een tekstverwerkingsdocument, folders, afbeeldingen, …
Sociale media	Elke vorm van publieke communicatie op het internet. Enkele voorbeelden van sociale media (let op, deze lijst is niet exhaustief): sites en apps van sociale netwerken (Facebook, Snapchat, LinkedIn, …), websites voor het delen van video's en foto's (Youtube, Instagram, …), blogs, forums of discussiegroepen (Reddit, Google Groups, …) , chatrooms, websites voor korte berichten (Twitter, …), websites voor gezamenlijk publiceren (Wikipedia, …), …
Chief Information Security Officer (CISO)	De persoon die beslist of al dan niet tot een controle wordt overgegaan, en aan wie IT-incidenten gemeld moeten worden. Cfr hoofdstuk 7. Bereikbaar via security@gial.be
ICT-dienstverlener	Diegene die ICT-middelen ter beschikking stelt of uitbaat in een contractuele relatie met de Stad.

HOOFDSTUK II.
MATERIAAL.

Artikel 2.- Aan elk personeelslid van de Stad worden een aantal standaard ICT-middelen ter beschikking gesteld, naarmate hun functie. Deze middelen blijven eigendom van de werkgever. Het personeelslid is verplicht goede zorg voor deze middelen te dragen.

Het personeelslid geeft in het geval van aflopen of stopzetten van zijn of haar tewerkstelling deze middelen, alsook al het bijhorende materiaal (tassen, etuis, etc.), terug aan zijn of haar (adjunct-)informaticacorrespondent of indien deze afwezig zijn aan het centraal secretariaat, en dit ten laatste op de laatst gepresteerde dag.

In geval van diefstal van materiaal is het personeelslid verplicht dit aan te geven aan de politie, en het proces-verbaal te bezorgen aan de directie Ontwikkeling en Organisatie.

Artikel 3.- Een aantal ICT-middelen worden gemeenschappelijk aan een deel of het geheel van het personeel ter beschikking gesteld. Ook hiervoor is het personeelslid verplicht zorg te dragen als goede huisvader.

HOOFDSTUK III.
GEBRUIK VAN ICT-MIDDELEN.

Artikel 4.- Alle onderstaande richtlijnen betreffende het gebruik zijn van toepassing op al deze middelen, alsook op eigen ICT-middelen wanneer het personeelslid ervan gebruik maakt in het kader van zijn of haar werk en tijdens de werkuren (privé computer via VPN, eigen smartphone, …).

Het personeelslid dat vanop afstand werkt is aan dezelfde richtlijnen onderworpen als wanneer hij of zij zich op de normale werkplaats bevindt.

Sectie I.- Professioneel gebruik.

Artikel 5.- Voor de richtlijnen betreffende een professioneel gebruik van ICT-middelen kan de directie strengere vereisten opleggen; het personeelslid is alleszins verplicht

Correspondentie	a) een officieel e-mailadres (onder bv. het domein brucity.be) te gebruiken voor elke correspondentie, intern of met buitenstaanders in het kader van zijn of haar functie; b) regelmatig zijn of haar inkomende post te bekijken, tijdig te antwoorden of eventueel te laten weten wanneer hij op zij pas gevolg zal kunnen geven aan het bericht; c) het aantal geadresseerden in e-mails te beperken tot het absoluut noodzakelijke; d) een bericht louter als ‘dringend’ te taggen indien dit echt nodig is; e) bij het foutief versturen van een e-mail te proberen deze e-mail te herroepen, of deze foutief geadresseerde in te lichten van zijn of haar vergissing; f) bij de ontvangst van een herroeping van een e-mail deze niet te openen en onmiddellijk te verwijderen;
Handtekening en lettertype	g) de gestandaardiseerde e-mailhandtekening en het gestandaardiseerde lettertype te gebruiken - deze worden vastgelegd door de cel Communicatie en zijn te raadplegen in het grafisch charter;

Out of office	h) bij afwezigheid van meer dan één dag een out-of-office bericht op te stellen (bij ziekte via webmail[1]) - in dit bericht wordt de periode van afwezigheid vermeld alsook de perso(o)n(en) of dienst die in dringende gevallen gecontacteerd kunnen worden;
Bijlagen van e-mails	i) te vermijden volumineuze bestanden in bijlage aan e-mails toe te voegen; j) naar een gedeelde map te verwijzen i.p.v. bestanden aan e-mails toe te voegen;
Printen	k) afdrukken van e-mails en documenten zo veel mogelijk te vermijden en de voorkeur te geven aan het projecteren en digitaal doorsturen ervan;
Archiveren	l) regelmatig zijn of haar mailbox op te kuisen en enkel berichten die nog kunnen dienen of niet verwijderd mogen worden in de mailbox te bewaren; m) zijn of haar mailbox te archiveren alvorens berichten en bestanden te verwijderen;
Kalender	n) zijn of haar Outlookkalender volledig in te vullen met de momenten waarop hij of zij niet beschikbaar is, en hiervoor een onderscheid te maken tussen momenten waarop hij of zij bezig of afwezig is;
Duurzaamheid	o) zijn of haar toestellen (schermen, pc's, …) uit te schakelen bij het verlaten van de werkpost, alsook de gedeelde toestellen (printers, elektronische borden, …) indien hij of zij als laatste de werkplaats verlaat.

Artikel 6.- Een disclaimer wordt automatisch toegevoegd aan verzending naar domeinen die niet rechtstreeks aan de Stad Brussel of haar ICT-dienstverlener verbonden zijn. Het personeelslid is verplicht deze intact te houden.

Artikel 7.- Het sturen van collectieve berichten aan al de leden van meerdere departementen of aan het geheel van het personeel van de Stad, is het voorwerp van een bijzondere procedure:

Aanvraag	a) De aanvragen voor verzending moeten verzonden worden naar het e-mailadres van de dienst Interne Communicatie van het Departement HR om na te gaan of, in functie van wat hier volgt, niets de verspreiding van dit bericht in de weg staat. Verder moet ook de verspreiding aan personeelsleden die niet gemakkelijk hun e-mailadres consulteren verzekerd worden, onder de verantwoordelijkheid van hun leidinggevende. b) De teksten die voorgelegd worden zullen voldoende goedgekeurd zijn door het betrokken departement/kabinet. De gegevens van de verantwoordelijke uitgever (dienst of persoon) zullen vermeld zijn, met inbegrip van het e-mailadres. c) Voor de berichten van categorie 2 tot 4 moeten de teksten ruim op voorhand bezorgd worden om de dienst Interne Communicatie de gelegenheid te geven de paginaopmaak en de verzending te verzorgen. Een minimale termijn van twee dagen is vereist.
Categorieën	d) De berichten zullen ingedeeld worden volgens hun belangrijkheid (voorbeelden): CAT 1: Organisatie van het werk = stroomonderbrekingen, technische interventies en onderhoudswerken aan het netwerk, de telefonie, enz., wijzigingen van het reglement; CAT 2: Werkaanbiedingen = oproepen tot mobiliteit, aanwerving, Selor, vormingen, ...; CAT 3: Gratis uitnodiging of voordeel voor het Stadspersoneel;

1 Bv. webmail.brucity.be

	CAT 4: Evenement = zuivere publiciteit (als er geen voordeel is voor de personeelsleden).
Inhoud	e) De aanvrager zal de tekst beperken tot maximaal 250 woorden per taal. Links naar intranet en internet zijn toegelaten. f) In de berichten zullen de namen van de schepenen vervangen worden door “Het College”.
Tweetaligheid	g) Volledige tweetaligheid (Frans/Nederlands) is van toepassing, zowel in de tekst van het bericht als in de eventuele bijlagen (.pdf, beeld met tekst, enz.). Rekening houdend met de wetgeving betreffende het gebruik van de talen zal de aanvrager, indien er verwijzingen zijn naar andere websites (Stad of andere), ook de links geven in de beide talen.
Bijlagen	h) De eventuele bijlagen dienen in veelvoorkomende formaten geleverd te worden, bv. .jpg (tekening of foto), .doc (Word), .xls (Excel), .pdf (Acrobat) en zeker niet uit gescande documenten te bestaan.
Verspreiding	i) In geval van verschillende, gelijktijdige aanvragen zal de dienst Interne Communicatie van het departement HR kunnen beslissen over de volgorde van verzending, om erover te waken de frequentie van één bericht per dag niet te proberen overschrijden. j) Indien niet anders aangeduid zal de verspreiding gebeuren aan het geheel van de personeelsleden van de Stad. Op aanvraag kan de verzending ook meer gericht gebeuren, zolang het groepen of lijsten betreft die voorzien zijn in Outlook; bv. “College”, “Departementen”, enz.
Opschorting, aanpassing of weigering.	k) De mails die te laat ontvangen worden of die niet stroken met de bepalingen van dit reglement mogen door de Dienst Interne Communicatie van het departement HR later verstuurd worden. Deze Dienst kan ook vragen de mail aan te passen aan het reglement en, indien dit niet gebeurt, de verzending van de mail weigeren.
Geen afwijkingen	l) Het is verboden dit soort berichten op een andere manier te versturen.

Sectie II.- Privégebruik.

Artikel 8.- Een redelijk privégebruik van ICT-middelen is toegestaan indien deze

a) infrequent en van korte duur is;
b) geen impact heeft op de plichten van het personeelslid of zijn of haar medewerkers;
c) geen impact heeft op de werking van de Stad;
d) geen extra kosten voor de Stad tot gevolg heeft;
e) niet in strijd is met andere onderdelen van deze policy;
f) niet in strijd is met de privacywet.

Ter informatie, enkele voorbeelden van toegestaan persoonlijk gebruik:	een eenvoudige online banktransactie uitvoeren; een korte persoonlijke e-mail opstellen; een kort telefoongesprek houden; uitzonderlijk enkele pagina’s afdrukken voor persoonlijk gebruik.
Ter informatie,	op uitgebreide wijze elektronische documenten voor persoonlijke doeleinden invullen;

enkele voorbeelden van niet toegestaan persoonlijk gebruik:	een boek kopiëren of uitprinten; telefoneren naar het buitenland; opzoekingen in beroepsapplicaties voor persoonlijke doeleinden.

Artikel 9.- Privégebruik van het professioneel e-mail adres kan indien het personeelslid de uitgaande e-mails als persoonlijk kenmerkt en het volgende toevoegt aan het bericht: “de inhoud van dit bericht is persoonlijk en kan in geen enkel geval leiden tot de aansprakelijkheid van de Stad Brussel”.

E-mails met een persoonlijk karakter moeten tevens bewaard worden in een Outlookmap met de titel “privé”, indien men wil dat de Stad deze e-mails niet kan consulteren.

Artikel 10.- Privégegevens mogen enkel worden opgeslagen in een folder genaamd “privé” op de lokale schijf (harde schijf van de pc), indien men wil dat de Stad deze gegevens niet kan consulteren. Deze folder mag geen professionele gegevens bevatten. In het geval van stopzetten of aflopen van het contract en/of teruggave van ICT-middelen is het personeelslid verplicht deze gegevens te verwijderen.

Sectie III.- Niet toegestaan gebruik

Artikel 11.- Het is voor het personeelslid verboden

Ongepaste inhoud	a) om websites te bezoeken, berichten te versturen of te beantwoorden met een inhoud die i. van erotische of pornografische aard is; ii. getuigend van racisme of vreemdelingenhaat is; iii. discriminerend op basis van geslacht, seksuele geaardheid, handicap, geloof, filosofische of politieke overtuigingen is; iv. revisionistisch is; v. pestgedrag of ongewenste intimiteiten bevattend of bevorderend is; vi. die niet respectvol tegenover anderen is; vii. of dergelijke meer dat in strijd met de goede zeden is of de waardigheid van anderen aantast;
Onwettig gebruik	b) om elke vorm van fraude, piraterij, hacken, online gokken, drugsverkoop, inbreuk op auteursrechten … of andere onwettige activiteiten aan te gaan;
Verspreiding van vertrouwelijke gegevens	c) om vertrouwelijke gegevens die betrekking hebben op de Stad, haar instellingen, personeelsleden, diensten, zakenpartners, klanten of andere belanghebbenden te verspreiden behalve in het kader van zijn of haar plichten; d) om inhoud te delen die beschermd is door de privacywet;
Frivool gebruik	e) om kettingmails te verspreiden, spelletjes te spelen, tijd in online chatrooms door te brengen, … en dergelijke meer; f) om langdurig muziek en/of video te streamen dat niet in het kader van het werk te plaatsen valt; g) volumineuze bestanden te downloaden;
Commercieel gebruik	h) om persoonlijke aangelegenheden met winstoogmerk aan te gaan, of reclame te maken voor belangen vreemd aan die van de Stad;
Laster	i) om de Stad, haar instellingen, diensten, personeelsleden, zakenpartners, klanten of andere belanghebbenden belasteren;

Verspreiding van eigen mening	j) de officiële handtekening te gebruiken in privécorrespondentie; k) om eigen meningen te laten voordoen als een officieel standpunt van de Stad, of ongeoorloofd in haar naam te spreken.

Artikel 12.- De werkgever weerhoudt zich het recht om op elk moment en zonder waarschuwing toegang tot bepaalde websites of bestanden te ontzeggen, voor de veiligheid van het informaticasysteem in het algemeen, of om een van bovenstaande verboden activiteiten te verhinderen.

Sectie IV.- Betreffende de sociale media.

Artikel 13.- Dit onderdeel van de policy slaat op het persoonlijk gebruik van sociale media, voornamelijk het **publiceren** van meningen, commentaren, foto's, statusrapporten of andere content, binnen de grenzen van artikel 8 omtrent privégebruik.

Specifieke regels betreffende het professioneel gebruik, d.w.z. de medewerkers die gemachtigd zijn om zich in naam van de Stad of uit te drukken of de Stad op sociale media te vertegenwoordigen, worden beheerd door de diensten Communicatie en maken geen onderdeel uit van deze policy.

In elk geval is het voor elk personeelslid die niet over dergelijke machtiging beschikt verboden om op sociale media actief te zijn terwijl hij of zij zich voordoet als de Stad of handelend in naam van de Stad. Het is het hem of haar wel toegestaan om in zijn of haar account de Stad als werkgever op te geven, mits vermelding dat het gaat om een persoonlijk account. Het is ook toegestaan om berichten gepubliceerd door de officiële accounts van de Stad te delen.

Artikel 14.- Alle richtlijnen uit deze policy betreffende het gebruik van ICT-middelen zijn ook van toepassing op het gebruik van sociale media op de werkplek of bij verplaatsing in het kader van zijn of haar werk of bij telewerken.

Bovenop deze richtlijnen is het de medewerker te allen tijde op sociale media, ook op persoonlijke ICT-middelen en buiten de werkuren, verboden om

Vertrouwelijke gegevens	a) vertrouwelijke gegevens die betrekking hebben op de Stad, haar instellingen, personeelsleden, diensten, zakenpartners, klanten of andere belanghebbenden te verspreiden;
Laster	b) de Stad en haar instellingen, personeelsleden, diensten, zakenpartners en andere belanghebbenden te belasteren;
Onjuiste gegevens	c) leugenachtige, misleidende of verwarring zaaiende uitspraken te doen betreffende de Stad en haar instellingen, personeelsleden, diensten, zakenpartners en andere belanghebbenden; d) zich voor iemand anders uit te geven die verbonden is aan de Stad; e) foutieve informatie inzake zijn of haar professionele ervaring of verantwoordelijkheden bij de Stad te publiceren;
Personeelsactiviteiten	f) foto's of video's van personeelsactiviteiten te posten zonder expliciete toestemming van de afgebeelde personen.

Artikel 15.- Aangezien het zo goed als onmogelijk is om een bericht dat via het internet gestuurd wordt te wissen wordt het personeelslid aangespoord goed na te denken alvorens via sociale media te communiceren of content van anderen via sociale media door te geven om geen inbreuk op de richtlijnen uit deze policy te plegen.

Het personeelslid moet zich er tevens van bewust worden dat zodra hij of zij content op sociale media plaatst hierover geen controle meer kan uitgeoefend worden, en het aantal personen die deze content gewaarworden of verder verspreiden niet meer kan ingeperkt worden.

Elk personeelslid is persoonlijk aansprakelijk voor de content die hij of zij op sociale media publiceert.

Artikel 16.- De werkgever weerhoudt zich het recht om de activiteiten van het personeelslid op sociale media te consulteren als ze betrekking hebben op de Stad, en desgevallend er gevolg aan te geven indien een inbreuk op bovenstaande regels betreffende het gebruik van sociale media wordt vastgesteld.

HOOFDSTUK IV.
COMPUTER- EN INFORMATIEBEVEILIGING.

Artikel 17.- Het personeelslid is verplicht

Integriteit	a) de herkomst en onschadelijkheid van bezochte websites en inkomend berichtenverkeer te verifiëren; b) het openen van spammails en onbetrouwbare bijlagen, alsook het downloaden van onbetrouwbare bestanden, zo veel mogelijk te voorkomen; c) te vermijden om te klikken op links in dergelijke onbetrouwbare mails, websites en bestanden;
Paswoorden en –beveiliging	d) een paswoord te kiezen dat niet gemakkelijk te raden is, en deze regelmatig te veranderen, en dat conform is met de paswoordpolicy;
Toegang tot de werkpost	e) bij het verlaten van zijn werkpost toegang tot zijn of haar computer en andere apparaten te vergrendelen;
Opslag	f) netwerklocaties te gebruiken voor de opslag van professionele bestanden in plaats van de harde schijf, tenzij het gaat over voorbereidende documenten; g) rekening te houden met het feit dat van de lokale schijf geen back-up gemaakt wordt.

Artikel 18.- Het is voor het personeelslid verboden

Paswoorden	a) zijn of haar paswoord te delen met anderen, zowel personeelsleden van de Stad als buitenstaanders (ICT-dienstverlener, consultants, vrienden, familie, …); b) het paswoord van een collega te vragen, ontvangen of gebruiken; c) een paswoord fysiek of digitaal te noteren; d) hetzelfde paswoord te gebruiken voor aan het beroep verbonden accounts als voor privéaccounts;
Toegang accounts	e) anderen, intern of extern, toegang te geven tot zijn of haar account; f) toegang tot de account van een collega te vragen, ontvangen of gebruiken;
Misbruik, sabotage of vandalisme	g) om misbruik te maken van ontdekte kwetsbaarheden in het systeem; h) om schade toe te brengen aan hardware, software, bestanden of processen, intern of extern, of deze ongeoorloofd te wijzigen of te verwijderen;
Software	i) om niet toegestane software te installeren of te gebruiken, d.i. software zonder de voorafgaande schriftelijke toelating van een meerdere of software die niet bedoeld is voor het uitoefenen van beroepsactiviteiten; j) willens en wetens uitvoerbare bestanden (bv. “.exe”) te activeren behalve met goedkeuring van de ICT-dienstverlener;
Hardware	k) om verwijderbare media aan te sluiten (USB-stick, smartphones, externe harddisk, …) tenzij de herkomst en inhoud gekend is ~~om verwijderbare media aan te sluiten tenzij de herkomst en inhoud gekend is~~;

	l) hardware materiaal dat niet ter beschikking werd gesteld door I-City, te verbinden met de computer, met uitzondering van randapparatuur die geen software installatie vereist (toetsenbord, muis, scherm, bluetooth headset…) en waarvoor het onderhoud niet wordt voorzien door I-City ~~eigen hardware materiaal (USB sticks, smartphones, …) te verbinden met de computer, tenzij deze op virussen werden gescand~~;
Opslag	m) om aan het werk gerelateerde bestanden op niet rechtstreeks aan het beroep verbonden clouddiensten (Dropbox, …) op te slaan; n) om aan het werk gerelateerde gegevens door te sturen naar een privéadres; o) om bestanden te verwijderen op gedeelde dossiers zonder expliciete goedkeuring van de eigenaar van het document (+ motivering waarom het document verwijderd moet worden);
Werken vanop afstand	p) zijn of haar pc en andere mobile devices onbewaakt en/of onvergrendeld achter te laten, in het bijzonder waar deze het doelwit van diefstal kunnen worden; q) om in publieke ruimtes om te gaan met vertrouwelijke informatie (bv. tegen meelezen); r) om afgedrukte pagina's met vertrouwelijke informatie mee naar huis te nemen, omdat deze moeilijk te beveiligen zijn.

Artikel 19.- Het personeelslid is bij het niet nauwgezet naleven van bovenstaande richtlijnen in elk geval persoonlijk verantwoordelijk voor ieder gebruik van zijn of haar account, door zichzelf of door anderen.

Artikel 20.- De werkgever weerhoudt zich het recht om met onmiddellijke ingang de toegang van het personeelslid tot zijn of haar account te herroepen.

HOOFDSTUK V.
VERANTWOORDELIJKHEID VAN HET PERSONEELSLID.

Artikel 21.- Van het personeelslid wordt verwacht kennis te nemen van de totaliteit van deze policy en deze na te leven.

Het personeelslid wordt door zijn of haar meerdere, of bij het aanwerven, gevraagd een kennisneming te ondertekenen.

Artikel 22.- Deze policy moet steeds worden geïnterpreteerd en toegepast met het oog op de goede werking van de diensten van de Stad en op de veiligheid van en zorg voor de ICT-middelen en netwerken van de Stad.

In het geval het personeelslid na het doornemen van deze policy niet zeker is of twijfelt over wat acceptabel gebruik van de ICT-middelen is, wat hij of zij niet mag doen of welke veiligheidsmaatregelen hij of zij moet nemen om de integriteit van het informaticasysteem niet aan te tasten, is deze verplicht om begeleiding en verduidelijking te vragen aan zijn of haar directie of (adjunct-)informaticacorrespondent.

Artikel 23.- Het personeelslid is verplicht, bij het vaststellen van een IT-incident qua computer- en informatieveiligheid in het kader van deze policy, onmiddellijk melding hiervan te maken aan de CISO (via security@gial.be) om verdere schade en verdere incidenten te vermijden. Dit zowel met betrekking tot zichzelf als tot zijn of haar medewerkers en werkomgeving. Het personeelslid wordt aangespoord op dat moment niets verder te ondernemen tot hij of zij toelating hiervoor gekregen heeft.

Artikel 24.- Overtreding van de richtlijnen van deze policy kan leiden tot disciplinaire procedures en sancties volgens het statuut.

HOOFDSTUK VI.
PRIVACY VAN HET PERSONEELSLID.

Artikel 25.- Alle ICT-middelen die de werkgever zijn personeelsleden ter beschikking stelt blijven eigendom van de Stad. Alle gegevens in elk dossier, bestand en/of e-mail, uitgegeven, ontvangen en/of bewaard zijn en blijven eigendom van de stad, tenzij deze duidelijk werden gekenmerkt als persoonlijk (zie hierboven omtrent privégebruik).

De Stad hecht groot belang aan het respecteren van de privacy van haar personeelsleden en leeft de privacywet nauwgezet na. Op het moment dat zij beslist om tot een controle over te gaan, engageert zij zich om dit te doen in overeenstemming met de finaliteits-, proportionaliteits- en transparantiebeginselen die deze wet voorschrijft (cfr. hoofdstuk 7).

Nota: De onderstaande procedures zullen worden herzien in het kader van de toepassing van de richtlijnen van de Algemene Verordening Gegevensbescherming die van toepassing zullen zijn op 25 mei 2018.

HOOFDSTUK VII.
MONITORING.

Artikel 26.- Op het moment dat een misbruik of verboden verbruik, d.i. een inbreuk op de veiligheidsmaatregelen en gebruiksrichtlijnen aangehaald in deze policy, wordt vermoed, kan het departementshoofd, hieronder genoemd de aanvrager van de controle, op vertrouwelijke wijze de CISO inlichten. Hierbij vermeldt hij expliciet en schriftelijk welk misbruik of verboden verbruik wordt vermoed.

Enkel de CISO kan beslissen om een verder onderzoek in te richten en het gebruik van de ICT-middelen te monitoren.

De Stad laat controles enkel in het kader van de hieronder beschreven beginselen uitvoeren en maakt in elk geval niet op permanente wijze gebruik van deze capaciteiten en voert geen voortdurende en systematische controles uit op het personeelslid.

Inbreuken die ontdekt worden bij het monitoren in het kader van een hoger doel kunnen de aanleiding zijn van onderstaande procedures.

Artikel 27.-

Finaliteitsbeginsel

De controle op het gebruik van de ICT-middelen kan enkel plaatsvinden indien een of meerdere van de volgende finaliteiten worden nagestreefd:

- de veiligheid en/of het goede werken van de informaticasystemen, alsook de materiele bescherming van het materiaal;
- het voorkomen van daden die onwettig of in strijd met de goede zeden zijn of de waardigheid van anderen aantasten;
- het eerbaar naleven van de gebruiksrichtlijnen betreffende de ICT-middelen zoals vermeld in dit document;
- de bescherming van de reputatie en de sociale en economische interesses van de Stad en haar instituties;
- de bescherming van de privacy, de waardigheid en de reputatie van haar personeelsleden en zakenpartners;
- de bescherming van de privacy van de burgers;

Proportionaliteitsbeginsel

Op het moment dat er een beslissing is om tot controle over te gaan, kan deze niet overgaan tot een systematische en oneindige inmenging, maar is deze beperkt tot een minimum en kan deze enkel

aanvullend plaatsvinden indien de aanvrager van de controle dit nodig acht middels een schriftelijk rapport.

Transparantiebeginsel

De controleprocedures worden bekendgemaakt aan het geheel van het personeel van de Stad via deze policy.

Artikel 28.- De verantwoordelijke van de uitvoering van deze controle is de ICT-dienstverlener. Deze heeft o.a. de technische capaciteit

- om een algemene lijst op te roepen van alle bezochte internetwebsites via haar netwerk, alsook de duur van het bezoek en het moment waarop dit bezoek plaatsvond;
- om betreffende het e-mailverkeer zaken zoals de frequentie, het aantal, de grootte, de bijlagen, … te monitoren;
- om per telefoon of fax de communicatiegegevens te bekijken zoals deze gefactureerd werden;
- …

De ICT-dienstverlener houdt zich aan een vertrouwelijke afhandeling van de gegevens en deze kunnen worden bewaard gedurende het onderzoek of de tijd noodzakelijk voor de verloop van een gerechtelijke procedure.

Op het moment dat de ICT-dienstverlener een afwijking vaststelt, informeert deze de CISO. Onder afwijking wordt verstaan elke inbreuk op de richtlijnen van deze policy. De afwijkingen worden formeel door de aanvrager van de controle vastgesteld, die een schriftelijk rapport opstelt.

Artikel 29.- De Stad weerhoudt zich het recht om, in het kader van de finaliteiten hierboven beschreven, over te gaan op de identificatie van het betrokken personeelslid. Deze controle kan louter resulteren in de identificatie van een personeelslid indien zij tot doel heeft:

- daden die onwettig of in strijd zijn met de goede zeden of de waardigheid van anderen aantasten te voorkomen;
- de economische en financiële belangen van de Stad te beschermen;
- de veiligheid of de werking van de computersystemen te verzekeren;
- elke andere inbreuk op de veiligheidsvoorschriften stop te zetten.

In andere gevallen, zoals bv. een inbreuk op de naleving van de gebruiksregels van ICT-middelen, kan een identificatie enkel plaatsvinden nadat eerst het personeel gezamenlijk gewaarschuwd werd dat een van deze regels overtreden werd, en een gelijkaardige overtreding opnieuw heeft plaatsgevonden.

Artikel 30.- Het personeelslid heeft het recht om

- tot een maand na het ingelicht worden van de controle alle informatie aan te vragen betreffende deze controle bij de CISO (recht op inzage);
- deze informatie door de CISO te laten vernietigen in het geval dat deze incorrect bleek of in strijd met de regelgeving van deze policy werd vastgelegd of meer dan één jaar oud is (recht op rectificatie en recht op gegevenswissing);
- tot een maand na het ingelicht worden van de controle bezwaar te maken tegen deze controle bij de Stadssecretaris (recht op bezwaar).

HOOFDSTUK VIII.
KWALITEITSTOEZICHT.

Artikel 31.- Een evaluatie van deze policy zal regelmatig en hoogstens jaarlijks worden gerealiseerd om bovenstaande richtlijnen te herzien in functie van

- nieuwe communicatiemiddelen en technologieën die gebruikt worden door de personeelsleden van de Stad;
- een evolutie van het wettelijk kader;
- het toetsen van de uitwerking en efficiëntie van de controleprocedures;
- het voor een andere reden noodzakelijk geacht worden door de werkgever of andere belanghebbenden.