HUISHOUDELIJK REGLEMENT VAN HET COLLEGE VAN BURGEMEESTER EN SCHEPENEN EN VAST BUREAU

De bepalingen van het huishoudelijk reglement zijn aanvullend op de bepalingen in het decreet over het lokaal bestuur.

Bijeenroeping

Artikel 1 - De gewone vergaderingen vinden wekelijks plaats op maandag om 13u30.

Indien de dag waarop de gewone zitting normaal plaatsvindt op een feestdag valt of het bestuur verhinderd is, kan de zitting die week op een ander tijdstip plaatsvinden of kan deze zitting geannuleerd worden.

Tijdens schoolvakanties kan er geopteerd worden om niet wekelijks te vergaderen.

Artikel 2 - De vergaderingen vinden plaats in een vergaderzaal van het lokaal bestuur

Artikel 3 – Het college van burgemeester en schepenen / het vast bureau kan digitaal vergaderen:

- indien de zaal niet beschikbaar is wegens een onvoorziene gebeurtenis (terreurdreiging, betoging, natuurramp, …)
- wanneer er sanitaire maatregelen van kracht zijn die het aantal contacten beperken
- indien 2/3de van de leden hiermee instemt

Artikel 4 – De digitale vergadering dient aan volgende voorwaarden te voldoen:

- ieder lid heeft afzonderlijk digitaal toegang tot de beraadslaging en de stemming
- de leden zijn zichtbaar en hoorbaar herkenbaar op een wijze waardoor hun identiteit kan worden vastgesteld
- bij een stemming over een onderwerp waarvoor geen geheime stemming is voorgeschreven, maakt ieder lid dat aan de vergadering deelneemt, zijn stem uitdrukkelijk kenbaar. De voorzitter controleert de authenticiteit van de uitgebrachte stem en maakt de uitslag onmiddellijk bekend.

Vastgesteld door het college van burgemeester en het vast bureau in zitting van 9 september september 2024

- bij een geheime stemming wordt de stemming op zodanige digitale wijze georganiseerd dat de voorzitter de authenticiteit van de uitgebrachte stem kan controleren, waarbij een geheime stem niet herleid kan worden tot het lid dat de stem heeft uitgebracht. De voorzitter maakt de uitslag onmiddellijk bekend.

Artikel 5 – In spoedeisende gevallen roept de burgemeester het college van burgemeester en schepenen samen voor een buitengewone vergadering, op de dag en het uur dat hij bepaalt.
In spoedeisende gevallen roept de voorzitter het vast bureau samen voor een buitengewone vergadering, op de dag en het uur dat hij bepaalt.

Informatie

Artikel 6 – De agenda van de zitting wordt in de loop van donderdag ter beschikking gesteld. Diensten kunnen naderhand enkel dossiers toevoegen mits akkoord van de algemeen directeur.

Artikel 7 - De leden van het college van burgemeester en schepenen / vast bureau kunnen de dossiers raadplegen via de webapplicatie Meetingmobile. Via deze webapplicatie kunnen zij een dossier aanduiden ter bespreking indien gewenst en eventueel commentaren toevoegen.

Artikel 8 - De notulen van de vergaderingen kunnen worden geraadpleegd op de webapplicatie Meetingmobile.

Artikel 9 – Het college van burgemeester en schepenen / het vast bureau kan medewerkers, burgers en externen horen om toelichting te verschaffen.

Quorum

Artikel 10 - Het college van burgemeester en schepenen / het vast bureau kan alleen beraadslagen of beslissen als de meerderheid van de leden aanwezig is. Indien er 30 minuten na de start van de vergadering onvoldoende leden aanwezig zijn om geldig te kunnen beraadslagen, wordt de vergadering verdaagd.

Vastgesteld door het college van burgemeester en het vast bureau in zitting van 9 september september 2024

Interne taakverdeling

Artikel 11 - Het college van burgemeester en schepenen / vast bureau is een collegiaal orgaan. De aangelegenheden die tot zijn bevoegdheid behoren moeten steeds onderworpen worden aan een collegiale beraadslaging en besluitvorming; zij zijn niet vatbaar voor delegatie aan een individueel lid, tenzij krachtens een uitdrukkelijke wettelijke bepaling.

Artikel 12 - Het college van burgemeester en schepenen / vast bureau voert evenwel onder zijn leden een interne werkverdeling door, waarbij aan ieder lid de bijzondere verantwoordelijkheid wordt opgedragen voor een bepaald onderdeel van het bestuur.

Gelet echter op het collegialiteitsprincipe is deze taakverdeling slechts een bestuursmaatregel van interne orde, enkel gericht op vereenvoudiging van de taken van het bestuur. Zij houdt geen overdracht in van bevoegdheden; evenmin verleent zij de betrokken schepen / lid vast bureau enige persoonlijke macht over de aangelegenheden die hem werden toevertrouwd.

De krachtens deze taakverdeling toegewezen bevoegdheden kunnen dan ook enkel werkzaamheden omvatten in verband met de voorbereiding en het onderzoek van zaken die aan het bestuur worden voorgelegd, zoals bv. de bijzondere bestudering van het dossier, de voorafgaande raadpleging van deskundigen en het verzamelen van inlichtingen, zonder dat het de betrokken schepen / lid van vast bureau is toegestaan zelf uitvoeringsmaatregelen te treffen of beslissingen te nemen die de gemeente of het ocmw binden. Hiertoe behoren ook de representatieve taken, waarbij de betrokken schepen / lid vast bureau het bestuur vertegenwoordigd bij vergaderingen of officiële plechtigheden.

Artikel 13 – Bevoegdheidsverdeling:

Bart Van Couwenberghe

- Natuur en Digitalisering (ICT-Smart City, Noord-Zuid en Ontwikkelingssamenwerking, Dierenwelzijn, Leefmilieu, Duurzaamheid en Afvalbeleid)
- Veiligheid
- Ambtenaar burgerlijke stand
- AGB

Vastgesteld door het college van burgemeester en het vast bureau in zitting van 9 september september 2024

Wim Bollaert

- Omgeving, Bestuurlijke Organisatie en Lokale Economie (Personeel, Intergemeentelijke Samenwerking, Financiën en Ruimtelijke Ordening, incl. Vergunningsbeleid)

Gerda Lambrecht

- Onderwijs en Cultuur (inclusief Kinderopvang, Erfgoed, Bibliotheek en Toerisme)

Lenn De Cleene

- Infrastructuur en Mobiliteit (Openbare Werken)
- Patrimonium

Els Nelen-Pauwels

- Samenleven (Sociaal Beleid, Jeugd, Senioren, Sociaal Woonbeleid, Sport, Communicatie en Participatie, voorzitter BCSD)

Uitvoering beslissingen

Artikel 14 – De administratie voert de genomen beslissingen uit. De opdrachten worden door de algemeen directeur of door de bevoegde schepen gegeven, in overleg met de algemeen directeur.

Geheimhouding

Artikel 15 – Diegene die het college van burgemeester en schepenen / het vast bureau bijwonen zijn tot geheimhouding van de bespreking verplicht.

Vastgesteld door het college van burgemeester en het vast bureau in zitting van 9 september september 2024

ICT-materiaal

Laptop

Artikel 16 – Voor mandatarissen wordt er een laptop, muis en draagtas voorzien die ter beschikking staan voor de duur van het mandaat. Deze laptop is voorzien van een officepakket, outlook en toegang tot meeting.mobile voor het raadplegen van de te behandelen agendapunten.

Artikel 17 – De mandataris krijgt een O365 basislicentie met desktop, web- en mobiele versie van Word, Excel, Powerpoint, Clipchamp, Teams en Outlook en toegang tot meeting.mobile voor het raadplegen van de te behandelen agendapunten en een e-mailadres van het lokaal bestuur ter beschikking (voornaam.naam@hove.be). Dit e-mailadres wordt steeds gebruikt voor alle communicatie vanuit het mandaat en zal ook gebruikt worden vanuit de organisatie om met de mandataris te communiceren. Daarnaast is er 1TB OneDrive-cloudopslag ter beschikking.
Indien men spam-mail of phishingmails ontvangt, dient de mandataris dit te melden aan de dienst ICT. Het is niet toegelaten om op deze mails te reageren. Bij beëindiging van het mandaat wordt de mailbox gedeactiveerd en na 3 maanden worden bestanden verwijderd.

Artikel 18 – Elke mandataris krijgt een persoonlijke toegang tot het netwerk via zijn digitale identiteit. Voor alle toepassingen die in de cloud staan of voor toegang tot het intern netwerk vanop afstand (thuis) gebeurt dit door middel van MFA of Multi Factor Authenticatie (vb: Itsme) gewerkt.

Artikel 19 – Software voor wordt uitsluitend door de ICT-dienst geïnstalleerd.
Hardware wordt steeds gekoppeld door de ICT-dienst na overleg.

Smartphone

Artikel 20 – Mandatarissen zijn in de mogelijkheid om een smartphone te krijgen aangekocht door het lokaal bestuur. De mandataris heeft de keuze om een smartphone van het bestuur te gebruiken of om de eigen smartphone te gebruiken met voorwaarde dat deze een dual sim heeft.

Artikel 21 – De algemeen directeur bepaalt voor de organisatie welke de noodzakelijke functionaliteiten zijn en tegen welke kostprijs. We werken hier kostenefficiënt: ons materiaal moet doen wat nodig is, maar we betalen niet extra voor bepaalde merken of gadgets. De smartphone moet steeds compatibel zijn met de software van het bestuur.
Voor de mandatarissen wordt dezelfde lijn aangehouden als voor het personeel.

Vastgesteld door het college van burgemeester en het vast bureau in zitting van 9 september september 2024

Artikel 22 – De smartphone van het bestuur kan niet ter beschikking worden gesteld van derden. Waar mogelijk wordt geconnecteerd met een vertrouwd wifinetwerk om de kosten via 4G te beperken. Hiervoor heb je een inlog nodig. Log nooit in op openbare netwerken.

Artikel 23 – Er wordt een telefoonnummer (sim-kaart) ter beschikking gesteld. De bijhorende kosten voor telefonie en dataverkeer zijn ten laste van het lokaal bestuur.

Artikel 24 – Gezien enkel kosten verbonden aan het mandaat ten laste zijn van het bestuur, waakt de mandataris erover privégesprekken en datagebruik via een eigen abonnement te laten verlopen.

Artikel 25 – Kosten voor gebruik in het buitenland worden slechts uitzonderlijk ten laste genomen door het bestuur mits motivatie (buitenlandse dienstreis, dringende noodzaak om vanuit het buitenland contact op te nemen, …).

Afspraken

Artikel 26 – Een smartphone en laptop met toegang tot gegevens van het bestuur dient met de nodige zorg behandeld te worden:

- bewaren op een droge plaats
- beschermen tegen beschadigingen
- up-to-date en beveiligd houden door middel van virus en malwarescan
- schermbeveiliging instellen na bepaalde tijd inactiviteit
- steeds voorzien toegangsbeveiliging met pincode, ontgrendelpatroon, vingerafdruk, ….
- Open geen links in mail, webpagina's en in SMS-berichten die niet vertrouwd zijn
- nooit automatisch verbinden met openbare wifi-netwerken
- nooit onbeheerd te worden achtergelaten
- niet gebruiken tijdens het besturen van een voertuig

Artikel 27 – De smartphone kan gebruikt worden om:

- Mailbox te raadplegen
- Foto's te maken
- Websites en sociale media (in overeenstemming met de desbetreffende bepalingen) te consulteren
- Data van het lokaal bestuur te consulteren

Artikel 28 – Het is verboden om illegale software en software uit niet-vertrouwde bronnen te downloaden.

Artikel 29 – Rooten en jailbreaken van een apparaat is verboden, dit vergroot de kans op illegale software of toegang:

- Jailbreak is het mogelijk maken van het draaien van niet goedgekeurde apps op een iOS apparaat, waardoor ook mailware gedraaid kan worden

Vastgesteld door het college van burgemeester en het vast bureau in zitting van 9 september september 2024

- Rooten is het proces dat het mogelijk maakt men meer rechten krijgt op het apparaat (android) en daardoor het complete besturingssysteem te wijzigen of te vervangen, en daarmee mailware introduceren en beveiligingsinstellingen te omzeilen.

Artikel 30 – Bij schade, verlies of diefstal van een bedrijfstoestel of een persoonlijk toestel dat voor het werk gebruikt wordt, zal dit steeds binnen de 4 uur gemeld worden aan de algemeen directeur en de DPO (informatieveiligheid@hove.be).
Bij diefstal wordt steeds door de mandataris aangifte gedaan.

Artikel 31 – Zorg ervoor dat de functie 'zoek mijn mobiel' steeds aanstaat op de smartphone zodat deze gebruikt kan worden bij verlies / diefstal.

Artikel 32 – Zorg ervoor dat de gegevens van de organisatie gewist kunnen worden bij verlies. Dat kan via Android apparaatbeheer.

Artikel 33 – De werkgever is verantwoordelijk voor het onderhoud en reparatie van de apparatuur. De daaraan verbonden kosten zijn voor rekening van het lokaal bestuur, tenzij geconstateerd wordt dat er sprake is van onzorgvuldig gebruik van de ter beschikking gestelde apparatuur. Bij vaststellen van onregelmatigheden (virus, malware, …) (ook op een eigen smartphone) dient steeds een incidentmelding te gebeuren bij ICT en DPO (informatieveiligheid@hove.be).

Artikel 34 – De mandataris is zelf verantwoordelijk voor de persoonlijke data die op het toestel staan (bij gedeeld gebruik mandaat – privé) en dient zelf de nodige stappen te ondernemen om regelmatig de data op een andere plaats te bewaren (back-up). De mandataris is zelf verantwoordelijk voor de installatie van het toestel en updates van zijn smartphone.

Gebruikstermijn

Artikel 35 – Bij aanvang van het gebruik wordt de gebruiksverklaring ondertekend.

Artikel 36 – Bij het beëindigen van het mandaat, zal de mandataris de laptop en smartphone terug bezorgen aan het bestuur. Indien de mandataris de laptop en smartphone niet terug overhandigt, zal hij de kostprijs betalen die berekend wordt op de afschrijving: per maand wordt er 1/36ste van de aankoopprijs in mindering gebracht. De minimale kostprijs is 1/36ste van de aankoopprijs.

Artikel 37 – De levensduur van een smartphone wordt op minimaal 36 maanden vastgelegd.

Vastgesteld door het college van burgemeester en het vast bureau in zitting van 9 september september 2024

Na 36 maanden kan het telefoontoestel vervangen worden. Indien het toestel echter nog performant is, wordt maar overgegaan tot vervanging indien de werking belemmerd wordt (trager functioneren, besturingssysteem is niet meer te updaten, …). Voor een laptop geldt eenzelfde regeling met een termijn van 72 maanden.

Artikel 38 – Indien een mandataris dit wenst, kan hij het door hem gebruikte ICT-materiaal overnemen bij beëindigen van het mandaat. De kostprijs hiervan wordt berekend op de afschrijving: per maand wordt er 1/36ste van de aankoopprijs in mindering gebracht. De minimale overnameprijs is 1/36ste van de aankoopprijs na 36 maanden.

Artikel 39 – Het gemengd gebruik (privé-mandaat) zal steeds worden aangegeven als voordeel van alle aard.

Artikel 40 – Het telefoonnummer wordt na afloop van een mandaat uit dienst genomen. De mandataris bezorgd hiertoe de sim-kaart terug.

Deconnectie

Artikel 41 – De mandatarissen zijn zich bewust van het deconnectiebeleid van het lokaal bestuur, dat berust op twee pijlers:

- Connectie

Connectie is de plicht van de medewerkers om tijdens de normale werkuren op een transparante manier beschikbaar en bereikbaar te zijn via de overeengekomen professionele communicatiekanalen binnen de geldende afspraken binnen de dienst, zij het persoonlijk dan wel op dienstniveau via back-ups.

In het geval van een dienstpermanentie, een noodtoestand of een dreigende aanzienlijke verstoring van essentiële dienstverlening die niet kan wachten tot de normale werktijden kan een medewerker alsnog worden gecontacteerd met inachtneming van de daarvoor voorziene compensaties.

- Deconnectie

Deconnectie is het recht van alle medewerkers om niet bereikbaar te zijn, geen e-mails, telefoontjes of werk gerelateerde berichten te ontvangen en te beantwoorden buiten de overeengekomen uren van bereikbaarheid, deze zijn in het flexcharter van de medewerkers bepaald van 9 tot 16u.

Een medewerker koppelt zo niet alleen fysiek los van de job, maar kan ook loskomen van werk gerelateerde informatie- en communicatietechnologieën.De werkgever mag je

dan ook niet meer contacteren tenzij er onvoorziene of specifieke omstandigheden zijn die niet kunnen wachten.

Artikel 42 – Voor dringende gevallen zijn er twee permanenties:

1. Voor technische interventies (openbaar domein, gebouwen, …) is de wachtdienst steeds bereikbaar op 0496/59 96 55.
2. Voor dossiergebonden materies is de algemeen directeur bereikbaar op 0491/61 45 77. Als zij afwezig is, is haar vervanger bereikbaar. Het bestuur wordt hier steeds over ingelicht.

Informatieveiligheidsbeleid & ICT-policy

Artikel 43 – Het informatieveiligheidsbeleid en ICT-policy heeft tot doel duidelijk te maken wat toegelaten is bij het gebruik van ICT-middelen. Hieronder verstaan we zowel hardware als software, alsook digitale communicatie.

Waarom is dit belangrijk?

- om risico's te voorkomen waardoor onder meer de continuïteit van de dienstverlening of de veiligheid van het netwerk in het gedrang komt
- de beschikbaarheid, integriteit en vertrouwelijkheid van informatie in het gedrang komt
- zorgen dat de verwerking van informatie niet in strijd is met de regelgeving betreffende de bescherming van persoonsgegevens.

Artikel 44 – Informatie is een bedrijfsmiddel dat, zoals andere belangrijke bedrijfsmiddelen, een grote waarde vertegenwoordigt en dus op gepaste wijze moet beschermd worden. De organisatie, de informatiesystemen en netwerken worden immers geconfronteerd met allerlei risico's die kunnen leiden tot problemen op het vlak van vertrouwelijkheid van gegevens, integriteit van gegevens en de beschikbaarheid van gegevens.

Artikel 45 – Op de werkplek zijn er verschillende documenten voorhanden die persoonsgegevens bevatten (namen, adressen, medische, raciale, religieuze, … gegevens). Deze gegevens moeten afgeschermd worden tegen ongeoorloofd gebruik door derden, wijzigingen en verlies van data.

Beheer van ICT-middelen

Artikel 46 – De gebruiker is verantwoordelijk voor de ICT-middelen die hem ter beschikking gesteld worden waarmee toegang tot informatie en gebouwen verkregen wordt. Dit betreft pc, laptop, smartphone, ipad, USB sticks, toegangsbadges, sleutels, … enzoverder. Dit is inclusief de toegewezen toegangscodes, gebruikersaccounts, wachtwoorden, … enzoverder. Deze ICT-middelen dienen in goede staat behouden blijven, mogen niet onbeheerd achtergelaten worden en worden beschermd om diefstal, beschadiging en misbruik te voorkomen.

Verwerking van persoonsgegevens

Artikel 47 – Iedereen wordt geacht de richtlijnen en procedures die van kracht zijn op het Vlak van de informatieveiligheid en privacy die uit dit beleid voortvloeien, na te leven.

De DPO wordt op de hoogte gebracht bij iedere schending van veiligheidsmaatregelen waarvan hij getuige is en van iedere onregelmatigheid die de beveiliging van de bedrijfsmiddelen in het gedrang kan brengen.

Hiertoe:

- gebruikt hij de bedrijfsmiddelen enkel voor de doeleinden waarvoor ze zijn bestemd en enkel in het kader van de toegangen die hem werden verleend;
- respecteert hij de instructies en richtlijnen die worden afgesproken in de uitvoering van dit beleid.
- is iedereen persoonlijk verantwoordelijk voor de aan hem toevertrouwde persoons- en andere gegevens krachtens het beroepsgeheim en de discretieplicht.

Inbreuken

Artikel 48 – Het is verboden de account van het bestuur te gebruiken voor (niet-limitatieve lijst):

- illegale of commerciële doeleinden
- bezoeken van websites die aanzetten tot
    - betrokkenheid bij illegale, frauduleuze of kwaadwillige activiteiten
    - laster en eerroof
    - het overtreden van de wet;
    - pesten op grond van geslacht, ras, nationaliteit, fysiek vermogen en andere
- bezoeken van websites met informatie die
    - een aanstootgevend, obsceen, pornografisch, raciaal of onterend karakter bevat
    - beledigend, kwetsend en/of bedreigend karakter bevat
- mededelen of downloaden van gegevens die met auteursrecht of copyright beschermd zijn;

- informatie vrij te geven die schade kan berokkenen onder andere aan de veiligheid van het land, de bescherming van de openbare orde, de financiële belangen van de overheid, het voorkomen en bestraffen van strafbare feiten, het medisch beroepsgeheim, de rechten en de vrijheden van de burger, de eerbiediging van de persoonlijke levenssfeer, enzovoort;
- verspreiden van vertrouwelijke informatie van het bestuur zonder dat dit nodig is voor een goede uitvoering van zijn taken;
- het ondernemen of deelnemen aan elke internetactiviteit (onder andere hacken) die bij wet verboden is;
- het gebruik van internet voor persoonlijk winstbejag;
- het deelnemen aan chatrooms, newsgroups, enzovoort, (tenzij ze nuttig en dienstig zijn voor de uitvoering van de taken), kettingbrieven en spammen;
- het bekijken of downloaden van zware bestanden (video's, films, online spelletjes, muziek,…);
- acties ondernemen die de beveiliging van systemen of informatie in het gedrang kunnen brengen zoals bijvoorbeeld interne en externe systeem- en netwerkbeveiliging omzeilen (virusscan uitschakelen,..)
- schadelijke software (bijvoorbeeld met gevaar voor virussen) op de computers van het bestuur installeren
- zich toegang verschaffen tot systemen waartoe men niet geautoriseerd is
- een valse identiteit aannemen op het netwerk
- andere gebruikers storen bij het uitoefenen van hun functie;
- persoonsgegevens te lekken of onrechtmatige toegang tot gegevens te verschaffen

Controle door werkgever

1. Toezichthoudend personeel

Artikel 49 – De controle op de naleving van de ICT-policy wordt toevertrouwd aan de ICT-coördinator, DPO en de algemeen directeur

2. Doel van de controle

Artikel 50 – Controle mag uitsluitend gebeuren met het oog op:

1° het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van een andere persoon kunnen schaden

2° de bescherming van de economische, handels- en financiële belangen van het bestuur die vertrouwelijk zijn alsook het tegengaan van ermee in strijd zijnde praktijken

3° de veiligheid en/ of goede technische werking van de ICT-netwerksystemen van de organisatie (vb: bestrijden van virussen), met inbegrip van de controle op de kosten die ermee gepaard gaan alsook de fysieke bescherming van de installaties van de onderneming

Vastgesteld door het college van burgemeester en het vast bureau in zitting van 9 september september 2024

4° controle op de toegang tot persoonsgegevens via loggings, waarmee kan achterhaald worden wie persoonsgegevens heeft geraadpleegd of bekendgemaakt.
5° het te goeder trouw naleven van de in de organisatie geldende beginselen en regels voor het gebruik van onlinetechnologieën, inclusief de richtlijnen i.v.m. informatieveiligheid

Artikel 51 – In eerste instantie mogen er enkel globale gegevens verzameld worden en is een identificatie van de individuele werknemers niet toegelaten.
Wanneer op basis van deze lijsten onregelmatigheden vermoed worden, kunnen deze lijsten verder worden geïndividualiseerd.
Wanneer een van de doelstellingen onder 1°,2°,3° of 4° wordt nagestreefd, kan direct worden overgegaan tot individualisering van de gegevens verkregen na controle.
Wanneer doelstelling 5° wordt nagestreefd, kan niet direct tot individualisering van de gegevens verkregen na controle worden overgegaan.

3. Controleprocedure

Artikel 52 – De controle op de onregelmatigheden gebeurt door de ICT-coördinator en de DPO. Deze rapporteert enkel aan de betrokken leidinggevende en de algemeen directeur over zijn bevindingen en is gebonden aan een geheimhoudingsplicht. De algemeen directeur zal, in kader van de controle op doelstelling 5°, per e-mail, de mandatarissen inlichten over het bestaan van een onregelmatigheid en over het feit dat de gegevens geïndividualiseerd zullen worden indien de onregelmatigheid blijft bestaan om verdere maatregelen te treffen.
Waar nodig licht de algemeen directeur de voorzitter van de gemeenteraad in, conform de bepalingen in de deontologische code van de mandatarissen, waarvan de bepalingen hierbij aanvullend zijn.

4. Inhoud van de controle

Artikel 53 – De aangewezen personeelsleden mogen elke controle uitvoeren of laten uitvoeren die inherent is aan het beheer van het informaticasysteem zelf, om de goede werking van het netwerk te waarborgen of om overbelasting of om veiligheidsproblemen te voorkomen.

Alle mandatarissen moeten zich bewust zijn van het bestaan van deze controlemogelijkheid en van het feit dat alle communicatie die zij via het netwerk uitwisselen, hieraan onderworpen kan worden. Ook een smartphone die gedeeltelijke gebruikt wordt voor privégebruik, kan gecontroleerd worden, voor wat betreft het gebruik en de data van de werkgever.

Vastgesteld door het college van burgemeester en het vast bureau in zitting van 9 september september 2024

Artikel 54 – De controle mag het gebruik van de elektronische communicatiemiddelen op een globale wijze nagaan. Zo mag een globaal overzicht van de gedurende een bepaalde periode bezochte websites alsook de frequentie en het volume van de doorgezonden informatie, zonder daarin op enige wijze gegevens over het individuele gebruik op te nemen.
Indien ze naar aanleiding van controletaken vaststellen dat een of meer gebruikers bewust of onbewust de veiligheid of de goede werking van het systeem in het gedrang brengen, mag hij deze gebruikers onmiddellijk identificeren en, indien nodig, contacteren om de problemen te verhelpen. Hij mag de activiteiten van deze gebruikers, indien noodzakelijk en na verwittiging, ook verder opvolgen om herhaling van het probleem te voorkomen.

Artikel 55 – Het gebruik van communicatiemiddelen in het bestuur wordt, buiten het zopas vermelde geval, niet systematisch op individuele wijze gecontroleerd.
Indien ze ongeoorloofd gebruik vaststellen dat een misdrijf uitmaakt of op ernstige wijze de financiële of economische belangen van het bestuur in het gedrang brengt, kunnen de betrokken gebruikers verder, zonder verwittiging, gecontroleerd worden met het oog op het verzamelen van bewijsstukken. Het bestuur zal meewerken bij het opsporen van dergelijke misdrijven, en zal eventuele gebruikersgegevens en bestanden overmaken aan de gerechtelijke instanties wanneer hierom verzocht wordt

Artikel 56 – De ICT-coördinator kan maatregelen treffen om ernstigere problemen te voorkomen. Indien er kosten verbonden zijn aan het verkeerd gebruik / misbruik van ICT-materiaal kunnen deze kosten verhaald worden op de mandataris.

Artikel 57 – Voor technische vragen i.v.m. ICT-middelen, wordt er contact opnemen met de ICT-coördinator.
Voor vragen over verwerken van persoonsgegevens en privacy wordt er contact opgenomen met de DPO.

Meldingsplicht in kader van incidentenprocedure

Artikel 58 – De mandataris dient de ICT-coördinator en DPO te informeren over:

- verdwenen informatie (ontbrekende bestanden, …)
- crashen van besturingssystemen
- software die niet naar behoren werkt
- het doorgeven van informatie aan derden zonder dat deze daar recht op hadden (of het vermoeden daarvan). Onder informatie verstaan we zowel bestanden, paswoorden, toegangscodes,…
- besmetting met virussen (onmiddellijk te melden om verspreiding tegen te gaan)
- het vermoeden dat anderen de ICT-policies niet naleven.
- Phishingmails / spamberichten
- Datalekken

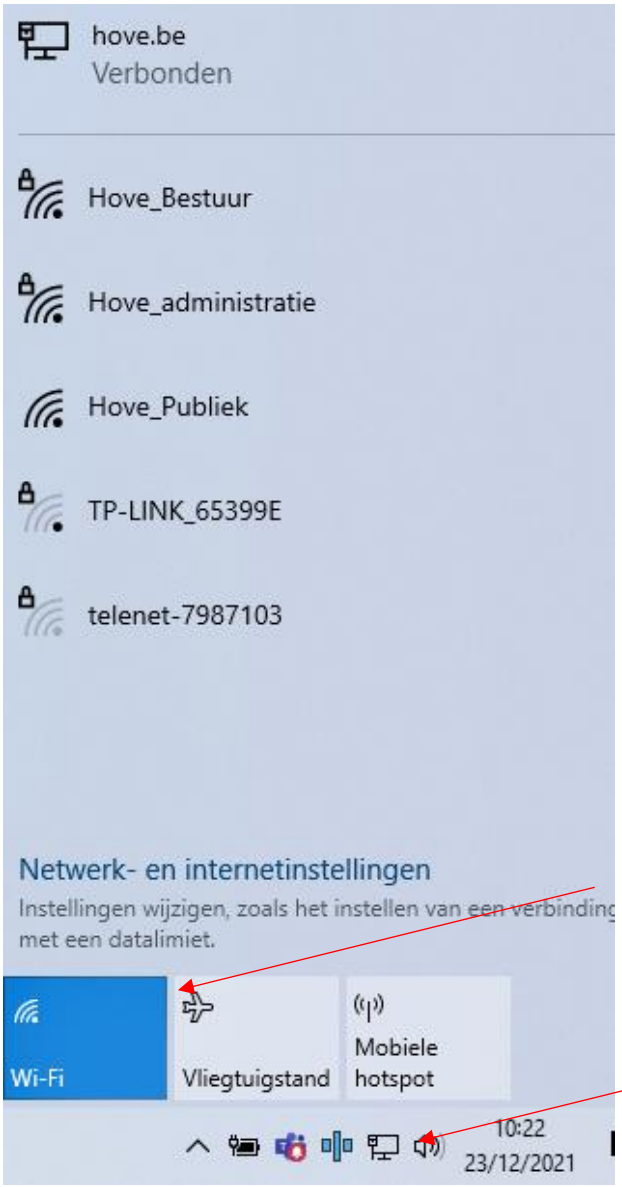
Vastgesteld door het college van burgemeester en het vast bureau in zitting van 9 september september 2024

- Inkijken van persoonsgegevens door onbevoegden en / of het verzenden van persoonsgegevens naar de verkeerde ontvangers

Artikel 59 – Alle gebruikers hebben de verantwoordelijkheid om inbreuken op deze gedragslijn te melden aan de ICT-coördinator en DPO via informatieveiligheid@hove.be

Wat te doen bij een cyberincident?

Artikel 60 – Bij een virusbesmetting of het binnenhalen van een criptolocker wordt de wifi uitgezet en wordt de netwerkkabel uitgetrokken. Let op: niet alles wordt uitgezet om zo de gegevens en bewijsmateriaal dat de security experts nodig hebben voor onderzoek te bewaren.
De wifi wordt uitgezet buiten de serveromgeving via instellingen. Hierna wordt de ICT-coördinator en de DPO zo snel mogelijk ingelicht.



Vastgesteld door het college van burgemeester en het vast bureau in zitting van 9 september september 2024

Data

Artikel 61 – Mandatarissen beschikken over een One-drive schijf waar ze hun gegevens kunnen opslaan.

Artikel 62 – Digitale informatie van externen wordt op een veilige manier in het netwerk overgezet. De informatie wordt opgeslagen in mappen, hierbij gebeurt er eerste een virusscan. Een USB-stick van derden om bestanden op te slaan wordt nooit gebruikt, hier zit geen virusscan op. Voor het opslaan wordt steeds de afzender nagekeken om zo de betrouwbaarheid van de bron na te gaan en om phishing te voorkomen. Bij twijfel wordt steeds de ICT-coördinator gecontacteerd.

Vertrouwelijke data kan alleen ingekeken worden indien er ingelogd wordt op de eigen server. Er worden geen gegevens van het bestuur thuis opgeslagen.

Clean desk

Artikel 63 – Clean Desk betekent een opgeruimde werkplek zonder rondsliggende papieren en een leeg scherm. Het scherm wordt steeds geblokkeerd (windowstoets+L) als je even niet aanwezig bent.

Artikel 64 – Er wordt gewerkt met een persoonlijke code voor de printer zodat er geen (al dan niet vertrouwelijke) informatie aan de printer kan blijven liggen. De fysieke aanwezigheid is vereist bij het printen tot na het printen.
Print enkel af als je een document echt op papier nodig hebt en laat geen afgedrukte papieren slingeren aan de printer.
Naast elke printer staat er een versnipperaar. Heb je documenten niet meer nodig? Haal ze door de versnipperaar.

Wachtwoordenpolicy

Artikel 65 - Op sommige toepassingen wordt een wachtwoordenpolicy automatisch opgelegd door de ICT-beheerder van het lokaal bestuur.
Voor andere toepassingen moet men zelf een wachtwoord instellen. Ook deze wachtwoorden dienen te voldoen aan de vereisten die de ICT-beheerder oplegt.
Welke regels volgen we?

- Gebruik nooit dezelfde wachtwoorden voor privézaken als voor je mandaat.

Vastgesteld door het college van burgemeester en het vast bureau in zitting van 9 september september 2024

- Een wachtwoord is strikt persoonlijk. Je zorgt ervoor dat het geheim blijft (niet ergens opslaan, niet delen, niet meekijken als iemand zijn paswoord wijzigt, …)
- Wanneer de computer de vraag stelt om het wachtwoord te bewaren op het scherm, moet er steeds negatief op worden geantwoord.
- Als je voor een applicatie zelf een wachtwoord moet kiezen, kies je steeds voor een sterk wachtwoord. Dat is een lang wachtwoord met minstens 13 karakters. Met hoofdletters, kleine letters, cijfers en een niet-alfanumeriek teken. Er bestaan computerprogramma's die alle mogelijke combinaties van letters en cijfers aan een duizelingwekkende snelheid uitproberen totdat ze de juiste combinatie gevonden hebben. Een dergelijk programma kan korte wachtwoorden in enkele minuten of zelfs seconden raden. Als je een lang wachtwoord moeilijk kan onthouden, kan je een wachtzin maken. Kies een zin die alleen voor jou betekenis heeft en die ook rare woorden, cijfers en speciale tekens bevat.

Artikel 66 - Wat dien je te melden?

- Indien je vermoed dat je wachtwoord niet meer geheim is, verwittig je de dienst ICT en de DPO én pas je dit aan.
- Als je vermoed dat je toegang hebt tot bestanden waartoe je geen toegang nodig hebt of geen toelating voor hebt, meldt je dit aan de dienst ICT en de DPO.

Artikel 67 - De schermbeveiliging moet met wachtwoord beveiligd zijn en moet ook steeds ingesteld staan zodat deze automatisch in werking treedt binnen de 5 à max. 10 minuten. Deze schermbeveiliging met wachtwoord volstaat echter niet om aan voorgaand artikel te voldoen. Ze fungeert enkel als noodoplossing voor het geval een gebruiker zelf vergeten is zijn pc te vergrendelen.

Vastgesteld door het college van burgemeester en het vast bureau in zitting van 9 september september 2024