

ICT - Gedragscode

Gemeente Zuidplas



Waarom een gedragscode?

Als je de krant leest of het journaal bekijkt zie je het regelmatig voorbijkomen: incidenten op het gebied van ICT en/of Privacy. We leven in een tijd waarin informatie en het gebruik daarvan razendsnel toeneemt. Dat kan heel handig zijn maar brengt ook grote risico's én verantwoordelijkheden met zich mee. Hoe ga jij als medewerker van Zuidplas hiermee om?

Zuidplas doet een beroep op je gevoel van eigenaarschap en verantwoordelijkheid, oftewel je morele kompas. Dat is best spannend omdat wij hiermee vertrouwen op jouw verantwoordelijkheidsgevoel zonder een pakket aan regels. Deze gedragscode helpt je daarbij.

NIET

Een dikke notitie vol juridische teksten of technische ICT-termen over wat wel en niet mag.

Waarschijnlijk lees je dat niet eens helemaal door en daarmee creëren we slechts een schijnveiligheid.

WEL

Een gedragscode over het juiste gebruik van ICT-middelen. Wij geven jou handvatten, tips en tricks zodat jij een beroep kunt doen op jouw eigenaarschap als professional.

ICT Middelen



Hoe ga je hier veilig mee om? Je leest het op pagina 2.

Informatie-veiligheid



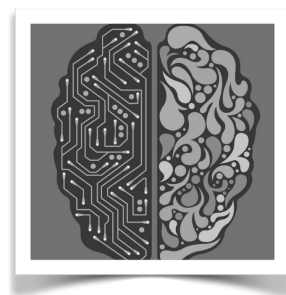
Op pagina 3 lees je welke onderwerpen van belang zijn op het gebied van informatieveiligheid

Tips & Tricks



Informatieveiligheid voor dummies op pagina 4

Je krijgt van de gemeente Zuidplas ICT-middelen ter beschikking om je werk goed uit te kunnen voeren. Wij vragen van jou deze ICT-middelen te gebruiken met gezond verstand. Om je daarbij te helpen geven wij je de volgende handvatten.



BIJ ICT-MIDDELEN GAAT HET OM

1. mobiele apparaten, zoals laptops, tablets en mobiele telefoons
2. pc's en telefoons in gebouwen van de gemeente Zuidplas
3. sleutels of elektronische tags voor toegang tot gebouwen of voorzieningen.



NIJWSTE VERSIE BESTURINGSSYSTEMEN

1. Zorg ervoor dat het besturingssysteem op je mobiele telefoon van de Gemeente Zuidplas up-to-date is. Via instellingen kun je zien of je telefoon is voorzien van de nieuwste software. Open verder regelmatig de bedrijfsportal app zodat je toestel voldoet aan het laatste beveiligingsbeleid.
2. Check één keer in de maand of je Chromebook is voorzien van de laatste software. Voer indien nodig een update uit



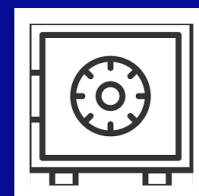
BIJ SCHADE, VERLIES OF DIEFSTAL

1. maak je een melding via het servicepunt. Bij verlies/diefstal is er sprake van een datalek, dus maak dan direct een melding.
2. In het geval van verlies/diefstal doe je binnen 24 uur aangifte bij de politie. Stuur een kopie van de aangifte naar het servicepunt.



VEILIG OPBERGEN

Wees alert op jouw mobiele devices. Verlies ze niet uit het oog of zorg ervoor dat devices goed zijn opgeborgen in een afgesloten ruimte of kast. In het bijzonder mogen devices niet in de auto worden achtergelaten.



INLEVEREN APPARATUUR

Apparatuur die niet meer wordt gebruikt of achterblijft wanneer de medewerker uit dienst gaat wordt ingeleverd bij het servicepunt. Het overnemen van apparatuur wordt niet toegestaan.

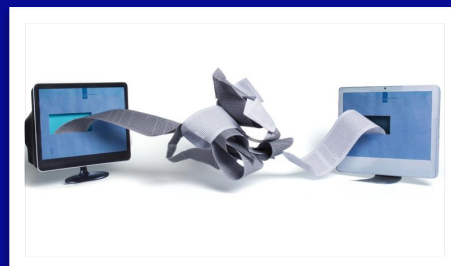


Jij bent als medewerker verantwoordelijk voor het veilig verwerken van (gevoelige) informatie. Daarom heeft de gemeente Zuidplas een aantal onderwerpen belicht die belangrijk zijn bij het werken met (gevoelige) informatie.



DATALEK

Als persoonsgegevens toegankelijk en of inzichtelijk zijn voor personen die geen toegang behoren te hebben tot deze gegevens, dan is er sprake van een datalek. Als je een datalek tegenkomt, meldt dit dan bij de FG. Als hij/zij afwezig is kun je ook terecht bij de CISO.



TOEGANG TOT INFORMATIE

Het raadplegen en wijzigen van informatie is alleen toegestaan als dit nodig is voor je werk. Je mag niet proberen toegang te krijgen tot vertrouwelijke informatie die niet voor jouw taken is bedoeld. Je mag dossiers die je niet nodig hebt voor je taken dus niet opzoeken of raadplegen. Ook niet als het naaste familie betreft.



WACHTWOORDEN

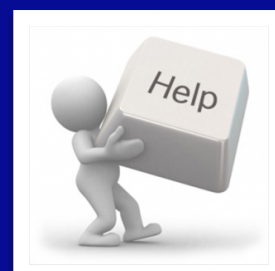
Wachtwoorden met namen van je partner, ouders en kinderen zijn makkelijk te onthouden maar daarom ook makkelijk te hacken. Ook tijdelijke wachtwoorden zoals Welkom01! en Zomer01! zijn populaire wachtwoorden onder hackers. Wachtwoordzinnen zijn veiliger dan wachtwoorden met hoofdletters. Een gewone zin - bijvoorbeeld "Frankie gaat altijd op de step naar huis" is veiliger dan een wachtwoord met hoofdletters, cijfers en tekens, én is ook nog eens gemakkelijk te onthouden. Wachtwoorden mogen niet worden opgeschreven of in een bestand worden opgeslagen. Maak zo veel mogelijk gebruik van een wachtwoordkluis (lastpass) en gegenereerde wachtwoorden.

Meest gelekte wachtwoorden

	Aantal
123456	6843
welkom	3115
welkom01	2770
wachtwoord	2057
qwerty	1863
amsterdam	1766
geheim	1740
123456789	1724
feyenoord	1247
12345	1071

TWIJFEL?

Als je twijfelt hoe je met bepaalde informatie moet omgaan, aarzel dan geen moment en vraag de CISO (Chief Information Security Officer) of de FG (Functionaris Gegevensbescherming) om advies. Advies over persoonsgegevens kun je ook altijd inwinnen op de site van de Autoriteit Persoonsgegevens: <https://autoriteitpersoonsgegevens.nl>



Wat kun jij doen om zo veilig mogelijk met informatie om te gaan? Soms zie je door de bomen het bos niet meer. Wij geven je een aantal tips die kunnen helpen om hier op een juiste manier mee om te gaan.



VERGRENDEL JE SCHERM

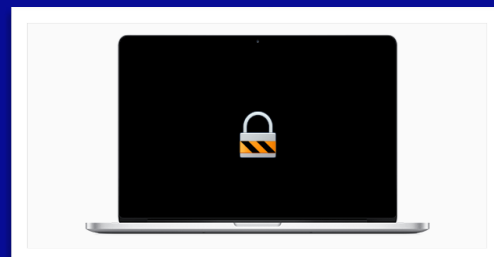
Zodra je je werkplek verlaat (let op: dit geldt ook voor de thuissituatie!). Dit kun je doen door middel van de volgende toetsencombinaties:



+ L (Thin Client)



+ L (Chromebook)



VEILIG MAILEN (BCC + ZIVVER)

Het openlijk gebruik van een emailadres van een burger is direct een datalek. Dit is een onderbelicht aspect maar niet onbelangrijk. Als je een email stuurt naar meerdere burgers tegelijk, gebruik dan altijd het 'BCC' plaats van 'Aan'. Een kleine moeite en op deze manier voorkom je een datalek.

Gebruik de Zivver applicatie voor het versturen van gevoelige informatie.



ETHIEK

Dit houdt in dat jouw werkzaamheden geen pornografisch, seksueel getinte, racistische, vernederende, discriminerende, beledigende en/of opruiende opmerkingen bevatten.



SOCIAL MEDIA

Je mag als medewerker berichten plaatsen over de Gemeente Zuidplas maar deze mogen niet in strijd zijn met gemeentelijk beleid. Beperk je tot het delen van informatie en vermijd discussie met inwoners.

Dit geldt zowel voor teksten als voor foto's, video- en geluidsopnamen.

Bij sociale media valt te denken aan: Facebook, LinkedIn, Twitter, Snapchat, Instagram et cetera.

