1. Wie is het bedrijf? Creativv
2. Contactgegevens: Creativv, Vliertwijksestraat 2 5249 RH Rosmalen, [www.creativv.nl](http://www.creativv.nl), info@creativv.nl 0638891729
3. Doel: Met welk doel verzamel je gegevens? Potentiële klanten kunnen contact opnemen voor meer informatie.
4. Wie gaan de persoonsgegevens ontvangen? Creativv
5. Hoe lang ga je de gegevens bewaren? 3 jaar
6. Na welke termijn ontvangt de bezwaarmaker geen email meer van de organisatie? Max. 12 maanden.
7. Inventariseer hoe je gegevens verzameld? Potentiele klanten vullen het contactformulier.
8. Bepaal welke gegevens je verzameld? Naam en emailadres
9. Zorg voor juiste beveiliging. Gegevens zijn beveiligd middels wachtwoorden die regelmatig worden gewijzigd

**Privacybeleid Creativv**

In het kader van de wet Algemene verordening gegevensbescherming (AVG). Dat betekent dat de privacywetgeving AVG geldt in de gehele Europese Unie.

Bedrijfsgegevens en contactgegevens

Creativv, Vliertwijksestraat 2 5249 RH Rosmalen, [www.creativv.nl](http://www.creativv.nl), info@creativv.nl 0638891729

Doel gegevens verzamelen

Potentiële klanten kunnen contact opnemen voor meer informatie.

Gegevens ontvangen en bewaartermijn

Creativv gaat de gegevens via de website ontvangen en de gegevens worden 3 jaar bewaard. Indien de gegevens niet meer nodig zijn, worden deze na 6 maanden verwijderd.

Gegevens verzamelen

Potentiele klanten vullen zelf het contactformulier in. Zij vullen de naam en het emailadres in.

Beveiliging

Gegevens zijn beveiligd middels wachtwoorden die regelmatig worden gewijzigd

Privacyreglement

U heeft het recht op inzage in uw gegevens, de mogelijkheid om uw gegevens te rectificeren of te wissen, u heeft het recht om tegen verwerking van gegevens bezwaar te maken. U heeft het recht om uw gegevens in te trekken. U heeft recht om beklag te doen bij de autoriteit persoonsgegevens: <https://autoriteitpersoonsgegevens.nl/>.

**Wilt u uw pc goed beveiligen, dan is antivirussoftware een goede eerste stap. Maar het is niet genoeg om uw pc echt veilig te maken, zeker niet wanneer het om een notebook gaat, die u wel eens meeneemt. Er zijn talloze andere maatregelen die u kunt nemen om de pc veilig te maken. In dit eerste deel van deze cursus leggen we uit hoe u met enkele basismiddelen uw systeem beveiligt.**

## Hoe veilig is veilig?

Hoe ver moet u gaan in het beveiligen van de computer en de gegevens daarop? En komt de grootste bedreiging via internet of e-mail, of bent u toch eigenlijk zelf verantwoordelijk, bijvoorbeeld omdat u niet regelmatig een back-up maakt? Beveiliging kunt u zo complex maken als u zelf wilt, maar er zijn relatief eenvoudige maatregelen die een grote bijdrage leveren aan het reduceren van risico's.

## 1. Een veilig besturingssysteem

Windows is verreweg het meest gebruikte besturingssysteem, en het is een prima basis voor een veilige pc. De veiligste versie van Windows is op dit moment de 64bit-editie van Windows 7. In vergelijking tot de 32bit-versie van Windows 7 én ten opzichte van eerdere versies zoals Vista en XP, beschikt Windows 7 x64 namelijk over een aantal aanvullende veiligheidsmaatregelen. Voorbeelden zijn een strengere controle van drivers en een Kernel Patch Protection, dat de Windows-kernel beschermt tegen wijzigingen. Beschikt uw pc over een 64bit-processor en minimaal 3 GB geheugen, gebruik dan de 64bit-versie van Windows 7. Om te zien of uw pc geschikt is klik op **Start** en typt u in het zoekvak het commando **msinfo32.exe** en drukt u op **Enter**. In het hulpprogramma Systeeminformatie kunt u dan bij **Systeemtype** zien of de pc een "Op x64-gebaseerde PC" is. Is uw pc dit niet, neem dan bij voorkeur de 32bit-versie van Windows 7.



**Controleer of uw pc geschikt is voor de 64bit-versie van Windows 7.**

## 2. Een schoon en up-to-date systeem

Een veilige pc begint bij een malwarevrij systeem. Wilt u écht veilig beginnen, dan kunt u Windows 7 schoon installeren op een tijdens de installatie geformatteerde harde schijf. Raadpleeg hiervoor de cursussen [Een frisse start met Windows 7 deel 1](http://computertotaal.nl/software/22874-een-frisse-start-met-windows-7-deel-1.html), [Deel 2](http://computertotaal.nl/software/23094-een-frisse-start-met-windows-7-deel-2.html) en [Deel 3](http://computertotaal.nl/software/23205-een-frisse-start-met-windows-7-deel-3.html). Gebruik bij voorkeur een Windows-installatieschijf met zoveel mogelijk updates en servicepacks al geslipstreamd. Windows Update zorgt er onder andere voor dat alle bekende gaten in het besturingssysteem worden dichtgetimmerd. Het is dan ook zeker aan te bevelen het systeem steeds bij te werken.

Zodra de installatie is afgerond installeert u alle updates, zowel de belangrijke als de minder belangrijke. Start hiervoor via **Alle programma's** de **Windows Update**. Klik op **Instellingen wijzen** en kies voor **Updates automatisch installeren** en schakel de twee opties daaronder ook in. Klik op **OK** om de wijzigingen te bewaren en klik dan op **Naar updates zoeken**. Start na het installeren de computer opnieuw op en herhaal het installeren van updates tot er geen nieuwe meer worden gevonden.



**Kies voor een Aangepaste installatie om een ook echt schone installatie uit te voeren.**



**Installeer alle updates voor het besturingssysteem.**

## 3. Installeer antivirussoftware

Geen pc kan zonder antimalwaresoftware. Er zijn meerdere goede keuzes te maken. [G Data AntiVirus 2012](http://computertotaal.nl/software/23286-g-data-antivirus-en-internetsecurity-2012.html) is de winnaar in onze [test van beveiligingssoftware](http://computertotaal.nl/tag/av2012/index.html)van dit jaar. Maar er zijn meer kwalitatief goede programma's en de verschillen zijn dit jaar kleiner dan ooit. Ook Bitdefender, F-Secure, Kaspersky en Norton konden onze goedkeurig wegdragen. Kiest u voor een uitgebreider Internet Securitypakket, dan raden wij [Kaspersky Internet Security](http://computertotaal.nl/software/23133-kaspersky-internet-security-2012-en-anti-virus-2012.html) aan. Installeer de beveiligingssoftware, update deze en laat daarna een totale systeemscan uitvoeren. Omdat u Windows schoon hebt geïnstalleerd zou er geen malware gevonden moeten worden. Wilt u nog gegevens terugzetten, bijvoorbeeld vanaf de usb-schijf, koppel deze dan nu aan de computer en laat de beveiligingssoftware ook die schijf volledig controleren voordat u de bestanden naar de computer terugzet.



**Controleer het systeem op malware en laat alle verontreinigingen opruimen.**

## 4. Gebruikersaccounts maken voor Administrator-taken

Veel onveiligheid wordt niet veroorzaakt door dieven of hackers, maar door gebruikers die fouten maken of die ­(onbewust) onveilige software installeren. Een sleutel in het beveiligen van de computer is het beperken van de rechten van de gebruikers, inclusief uzelf. Dit kan door bij standaardgebruik van de pc niet als administrator in te loggen, maar als standaardgebruiker. Open via **Start** het **Configuratiescherm**. Klik op **Gebruikersaccounts en Ouderlijk toezicht** / **Gebruikersaccounts toevoegen of verwijderen**. U ziet uw eigen account dat tijdens de installatie van Windows is aangemaakt en dat administratorrechten heeft. Klik op **Een nieuw account maken** en geef het account uw eigen naam met als toevoeging Admin. Kies als type **Administrator** en bevestig via **Account maken**. Klik daarna op het nieuwe account en kies **Een wachtwoord instellen** en bescherm het met een wachtwoord. Keer terug naar **Accounts beheren** en zie dat er nu twee accounts zijn, beide met administratorrechten. Controleer het nieuwe account door via **Start** naast Afsluiten op de pijl te klikken en te kiezen voor **Afmelden**. Klik dan in het aanmeldscherm op het nieuwe Admin-account en controleer het wachtwoord door in te loggen.



**Maak eerst een tweede administratoraccount aan, om daarna uw eigen account tot een standaardaccount te degraderen.**