



# Veilig Online

Dienstbeschrijving

## Inhoudsopgave

1	Inleiding.....	3
2	Internet Veiligheidspakket.....	4
2.1	Beschrijving van de dienst.....	4
2.2	F-Secure (partner Internet Veiligheidspakket).....	4
2.3	Functionaliteit.....	5
2.3.1	Virus- en spywarebeveiliging.....	5
2.3.2	Internet Shield.....	5
2.3.3	URL-filter/blokking.....	5
2.3.4	Spambeveiliging.....	6
2.3.5	Serverbeveiliging <sup>1</sup> .....	6
2.3.6	Beveiliging van mobiele apparatuur <sup>1</sup> .....	6
2.3.7	Beheerportaal.....	6
2.3.8	Automatische updates.....	6
2.3.9	Overzicht van pakketten.....	7
2.4	Waarom heeft u het Internet Veiligheidspakket nodig?.....	8
3	Voordelen van Internet Veiligheidspakket.....	9
3.1	Ondersteunde besturingssystemen.....	9
3.1.1	Systeemeisen.....	9
4	Service Level Agreements.....	12
4.1	Openingstijden Business Servicedesk.....	12
4.2	Beschikbaarheid.....	12
4.3	Onderhoudsvenster.....	12
5	Helpdesk en procedures.....	13
5.1	Openingstijden Business Servicedesk.....	13
5.2	Communicatie over onderhoudswerkzaamheden.....	13
6	Tarieven en facturering.....	14
6.1	Tariefstructuur.....	14
6.2	Facturering.....	14
6.3	Contractduur.....	14
7	Back-up Online.....	15
7.1	Voordelen van Back-up Online.....	15
7.2	Functies van Back-up Online.....	15
7.3	Ondersteunde besturingssystemen.....	15
7.4	Bewaaropties.....	16
7.5	Advisering.....	16
7.6	Beveiligingsaspecten.....	16
7.7	Abonnementsvormen.....	16
7.8	Bestelwijze.....	17
7.9	Beschikbaarheid.....	17
7.10	Uitgangspunten.....	17
8	CyberCenter.....	18
8.1	Fysieke toegangsbeveiliging.....	18
8.2	Ruimte, lokale bekabeling en stroomvoorziening.....	18
8.3	Aarding en bescherming tegen elektrostatische ontladingen.....	18
8.4	Klimaatbeheersing en brandveiligheid.....	18
9	Informatiebeveiliging.....	19
9.1	De ISO 27001 en ISO 27002 richtlijn hoe te implementeren.....	19
9.2	Continuïteitsbeheer.....	19
9.3	Beveiligingsmaatregelen.....	19

## 1 Inleiding

Veilig Online is een bundel van twee producten: het Internet Veiligheidspakket en Back-up Online van KPN. In dit document vindt u een beschrijving van beide diensten.

## 2 Internet Veiligheidspakket

Deze dienstbeschrijving maakt samen met de Algemene Voorwaarden Software Online en de aanvullende licentievoorwaarden van F-Secure deel uit van alle overeenkomsten voor levering van het Internet Veiligheidspakket. KPN behoudt zich het recht voor om een nieuwe versie van deze dienstbeschrijving uit te brengen. In dat geval blijft de onderhavige versie van toepassing op alle lopende overeenkomsten die op basis van deze versie zijn aangegaan.

### 2.1 Beschrijving van de dienst

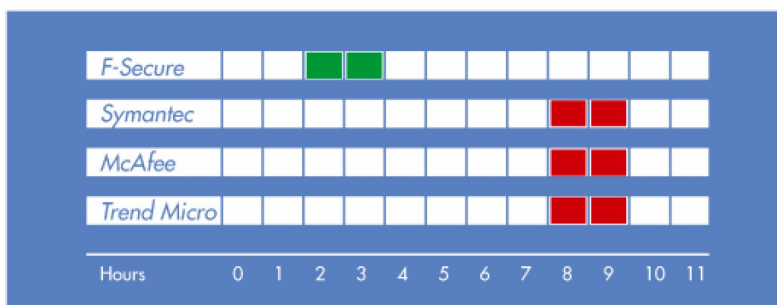
Modern zakendoen is sterk afhankelijk van computers. Toch beschikken veel kleine en middelgrote bedrijven nog steeds niet over een effectieve beveiligingsoplossing die hun bedrijfsmiddelen beschermt. In het ergste geval kunnen hierdoor waardevolle gegevens verloren gaan als gevolg van aanvallen van hackers en andere indringers. Als een bedrijf een vrijplaats voor spammers wordt, kan dit leiden tot diefstal van gegevens en verlies van omzet en kan de reputatie van een bedrijf zelfs ernstige schade oplopen.

Internet Veiligheidspakket is een abonnementsdienst waarbij u steeds beschikt over de meest recente versie van de software. U betaalt elke maand een vast bedrag en hoeft dus geen grote investeringen te doen

Met het Internet Veiligheidspakket biedt KPN u een nieuwe en gemakkelijke manier om uw bedrijf optimaal te beschermen tegen bedreigingen: een complete oplossing bestaande uit beveiligingssoftware en een beheerportaal. Het Internet Veiligheidspakket bestaat uit virus- en spywarebeveiliging, Internet Shield en URL-filter om volledige bescherming te garanderen – zelfs buiten de firewall van uw bedrijf. De ingebouwde spamdetectie zorgt ervoor dat uw e-mailverkeer gevrijwaard blijft van junkmail en andere ongewenste berichten.

### 2.2 F-Secure (partner Internet Veiligheidspakket)

F-Secure heeft een bewezen staat van dienst als het gaat om snel reageren op nieuwe bedreigingen. Het bedrijf is de markt telkens een stap voor in het ontwikkelen van software met bescherming tegen nieuwe schadelijke invloeden (malware). Snelheid is belangrijk – hoe sneller u beschermd bent, des te kleiner de kans dat u tegen problemen oploopt. Er verschijnen namelijk voortdurend nieuwe bedreigingen die zich razendsnel verspreiden.



## 2.3 Functionaliteit

Het Internet Veiligheidspakket is door F-Secure en KPN ontwikkeld en bevat een volledig geïntegreerde bescherming tegen virussen en spyware, een persoonlijke firewall, URL-filter, pop-upblokkering en spamfilter, waarmee u uw bedrijf eenvoudig in één keer kunt beschermen tegen internetbedreigingen. De functies van het Internet Veiligheidspakket worden hieronder toegelicht.<sup>1</sup>

### 2.3.1 Virus- en spywarebeveiliging

Virus- en spywarebeveiliging detecteert en blokkeert schadelijke software (malware) die uw computer kan aanvallen via e-mail, via verwisselbare media, of wanneer u materiaal van internet downloadt. Het beschermt uw privacy door geïnstalleerde gegevensverzamelende software van uw computer te verwijderen. Virus- en spywarebeveiliging:

- Plaatst reeds op uw computer geïnstalleerde schadelijke software 'in quarantaine' en verwijdt deze
- Blokkeert opdringerige reclame-popups
- Beschermt uw systeeminstellingen
- Detecteert potentieel schadelijke software (riskware) en plaatst deze in quarantaine of verwijdt deze

Het antivirus-onderzoekscentrum publiceert en ververst dagelijks de virusdefinities. Gebruikers ontvangen automatisch de nieuwste virusdefinities en updates van de spyware-database.

### 2.3.2 Internet Shield

Internet Shield beschermt uw computer tegen ongeautoriseerde pogingen om een verbinding tot stand te brengen, interne aanvallen, informatiediefstal, kwaadaardige applicaties en andere ongewenste applicaties, zoals peer-to-peer-software. De firewall is een belangrijk onderdeel van Internet Shield. Wanneer Internet Shield op uw computer geïnstalleerd is, beschikt u over firewallbescherming, zelfs wanneer u niet op het lokale bedrijfsnetwerk bent aangesloten. Wanneer een internetverbinding geactiveerd is, wordt de firewallsoftware automatisch bijgewerkt.

### 2.3.3 URL-filter/blokkering

Met deze functie kunt u toezicht uitoefenen om te voorkomen dat uw medewerkers toegang hebben tot ongeschikte informatie op het internet, zoals gewelddadig of seksueel getint materiaal. U kunt instellen hoeveel vrijheid medewerkers hebben bij het gebruik van internet op hun computer. Zo vermijdt u dat medewerkers op ongepaste websites terechtkomen. Met deze vorm van toezicht bepaalt u tevens het wachtwoord waarmee u de instellingen van het Internet Veiligheidspakket kunt wijzigen en waarmee u het toezicht op uw medewerkers beheert.

N.B.: Met het beheerportaal kunt u alle apparaten die voorzien zijn van het Internet Veiligheidspakket op afstand beheren en richtlijnen voor internetgebruik op deze apparaten implementeren.

### 2.3.4 Spambeveiliging

De spambeveiligingsfunctie bewaakt inkomende e-mailberichten en verwijdert ongevraagde e-mails (spam) uit uw postvak. Zodra een e-mail als spam wordt herkend, wordt deze als zondanig aangemerkt en in een afzonderlijke map geplaatst.

### 2.3.5 Serverbeveiliging<sup>1</sup>

Naast de beveiliging van werkstations maakt de beveiliging van servers ook deel uit van de dienstverlening. De servers worden net zoals de werkstations beveiligd tegen internetgerelateerde bedreigingen. De serverbeveiliging omvat zowel virus- als spywarebescherming.

De serverbeveiliging wordt geleverd vanaf pakket 2 (zie paragraaf 2.3.9).

### 2.3.6 Beveiliging van mobiele apparatuur<sup>1</sup>

Mobiele apparatuur met geavanceerde mogelijkheden zoals internet en e-mail wordt in toenemende mate standaard binnen veel bedrijven. Deze apparaten zijn niet alleen vaak verbonden met het internet, ze staan onderling ook met elkaar in verbinding, bijvoorbeeld via Bluetooth. Daarmee zijn mobiele apparaten net zo kwetsbaar voor hackers, spyware en virussen als normale pc's. KPN verwacht dan ook dat deze kwetsbare apparatuur in toenemende mate het slachtoffer wordt van diverse vormen van malware.

Om deze reden heeft KPN de beveiliging van mobiele apparatuur opgenomen in zijn dienstverlening. De beveiliging wordt verleend in de vorm van software die u op uw mobiele apparaat installeert en die uw apparaat automatisch beschermt tegen bedreigingen. Ook de software op uw mobiele apparaat wordt automatisch voorzien van de nieuwste updates. De beveiliging bestaat uit anti-virussoftware en een firewall.

### 2.3.7 Beheerportaal

Het beheerportaal is een website waarmee u uw licentiecodes kunt beheren. Alle door u aangevraagde licenties worden automatisch opgenomen in het portaal, zodat u op elk moment kunt zien wat de huidige status van uw licenties is. U kunt bijvoorbeeld controleren of bepaalde installaties al uitgevoerd zijn, of de software van de meest recente updates is voorzien, of alle programma-onderdelen geactiveerd zijn en welke profielen toegepast zijn. Daarnaast kunt u vanuit het beheerportaal de profielen op de lokale installaties toepassen.

Het beheerportaal wordt geleverd vanaf pakket 2 (zie paragraaf 2.3.9).

### 2.3.8 Automatische updates

F-Secure verzorgt voor KPN de hosting van de updatedienst van de beveiligingssoftware en onderhoudt deze. Wanneer eindgebruikers van de beveiligingssoftware verbinding maken met het internet, controleert de updatedienst op mogelijke wijzigingen van de productconfiguratie, de beschikbare software-, beveiligings- en profielupdates, en de beveiligingsprofielen en -upgrades. Eindgebruikers met een geldig abonnement ontvangen de updates, upgrades en nieuwe beveiligingsprofielen automatisch.

Versie 1.0<sup>1</sup> Omdat u altijd voorzien bent van de laatste software-updates kunnen er tijdens de looptijd van uw abonnement functies toegevoegd worden aan de dienstverlening. De meest recente beschrijving kunt u vinden op [kpn.com](http://kpn.com), trefwoord 'Internet Veiligheidspakket'.

### 2.3.9 Overzicht van pakketten

	Pakket								
Internet Veiligheidspakket*	1	2	3	4	5	6	7	8	9
Aantal te beveiligen apparaten									
Pc's	2	5	10	20	30	40	50	75	100
Smartphones	1	5	10	15	20	25	30	40	50
Servers	Nee	5	10	20	30	40	50	75	100
Beheerportaal	Nee	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

\* U kunt uw abonnement alleen opwaarderen naar een uitgebreider pakket, een downgrade is niet mogelijk.

Internet Veiligheidspakket	Virus- en spywarebescherming	Internet Shield	URL-filter	Spambeveiliging	Firewall
Pc-beveiliging	Ja	Ja	Ja	Ja	Ja
Serverbeveiliging	Ja	n.v.t.	n.v.t.	n.v.t.	n.v.t.
Beveiliging van mobiele apparaten	Ja	n.v.t.	n.v.t.	n.v.t.	Ja

## 2.4 Waarom heeft u het Internet Veiligheidspakket nodig?

- 80 procent van de kleinzakelijke computergebruikers gebruikt apparatuur die besmet is met spyware en/of adware
- 67 procent van de eindgebruikers beschikt niet over actuele antivirussoftware
- 82 procent van alle binnenkomende e-mailberichten bestaat uit spam
- Er worden elke dag zo'n 10 tot 15 nieuwe computervirussen ontdekt
- Er bestaan op dit moment meer dan 185.000 computervirussen

### 3 Voordelen van Internet Veiligheidspakket

De voordelen van het Internet Veiligheidspakket zijn duidelijk. Uw beveiliging wordt kundig en efficiënt verzorgd, zodat u zich volledig op uw bedrijf kunt richten.

- Voordelige abonnementsstarieven
- Aan te passen aan uw zakelijke behoeften dankzij handige product- en licentiecombinaties
- Eenvoudig installatiebeheer en flexibel gebruik van licenties (direct overzicht van de licentie- en installatiestatus) door middel van beheerportaal
- Eenvoudig te installeren via de webpagina van kpn.com
- Complete beveiligingsoplossing inclusief virus- en spywarebeveiliging, Internet Shield, spamdetectie en URL-filter
- Minimale onderhoudsinspanningen vereist: automatische updates van virusdefinities en software-upgrades worden automatisch gedownload
- Vooraf opgestelde beveiligingsprofielen voor verschillende gebruikersgroepen met uiteenlopende behoeftes
- Bescherming van uw kwetsbare mobiele apparatuur
- Ondersteuning door KPN bij eventuele problemen

#### 3.1 Ondersteunde besturingssystemen

Het Internet Veiligheidspakket ondersteunt de onderstaande besturingssystemen:

- Windows 2000 Professional SP4
- Windows XP Professional of Home Edition SP2
- Windows Vista (32-bit)
- Windows Server 2000 en 2003

##### 3.1.1 Systeemeisen

Uw computer moet aan de volgende eisen voldoen om het Internet Veiligheidspakket te kunnen installeren en uit te voeren:

Internet Veiligheidspakket voor werkplekken

- Besturingssysteem: Windows 2000-SP4 / XP / Vista 32-bit
- Processor: Intel Pentium III, 600 Mhz of hoger
- Geheugen (minimaal): Windows 2000 / XP 256 MB (aanbevolen: 512 MB), Windows Vista 512 MB (aanbevolen: 1 GB)
- Schijfruimte: 500 MB vrije schijfruimte
- Beeldscherm: minimaal 8-bit (256 kleuren)
- Internetverbinding: een internetverbinding is noodzakelijk om virusinformatie en updates te ontvangen
- Browser: Internet Explorer 6.0 of hoger

### Internet Veiligheidspakket voor servers

- Besturingssysteem: Microsoft Windows 2000 Server, Windows Server 2003
- Processor: Intel Pentium III, 800 Mhz of hoger
- Geheugen: 512 MB
- Schijfruimte: 300 MB vrije schijfruimte
- Beeldscherm: minimaal 8-bit (256 kleuren)
- Internetverbinding: een internetverbinding is noodzakelijk om virusinformatie en updates te ontvangen
- Browser: Internet Explorer 6.0 of hoger

N.B.: De minimale vereisten hebben betrekking op software die wordt gebruikt in een verder 'leeg' besturingssysteem waarin alleen primaire software is geïnstalleerd (browser, e-mail, etc.).

### Internet Veiligheidspakket voor mobiele apparaten

Het Internet Veiligheidspakket voor mobiele apparaten wordt ondersteund door de onderstaande mobiele apparaten. Voor de meest recente lijst van ondersteunde apparaten kunt u kijken op <http://mobile.f-secure.nl/kpn>.

#### UIQ:

Sony Ericsson P1i, W950i, M600i, P990i, W960i.

#### S60 2nd Edition (Symbian 7.x/8.x)

Nokia 3230, 6260, 6600, 6630, 6670, 6680, 6681, 6682, 7610, N70, N72, N90, Panasonic X700, Panasonic X800.

#### S60 3rd Edition (Symbian 9.x)

Nokia 3250, 5500, 5700, 6110, 6120, 6290, E50, E51, E60, E61, E61i, E62, E65, E70, E90, N71, N73, N75, N76, N77, N80, N81, N82, N91, N92, N93, N93i, N95, N95 8GB.

#### Windows Mobile 5.0 for Pocket PC (ondersteunt ook apparaten zonder telefoonfunctionaliteit)

- Dopod 838, Dopod 900, Dopod 818 Pro
- HTC Prophet, HTC P3300, HTC P3350, HTC P3600, HTC P3300, HTC P3600, HTC P4350, HTC X7500 (Athene)
- TyTN, HTC Universal, HTC Wizard, HTC X7500
- I-mate K-JAM, I-mate JASJAR, I-mate JAMin
- O2 Germany XDA neo, O2 Xda Atom, O2 Xda Exec, O2 XDA Mini S
- Qtek 9000, Qtek 9100, Qtek S200, Qtek v1640
- SPV M3000, SPV M5000, SPV M600
- T-Mobile MDA, MDA Pro, MDA Vario
- Asus P525, Cingular 8125, Gigabyte g-Smart, I-mate JAMin, Treo 700W, UBIQUIo 401, Palm Treo 750W, Toshiba Portégé G900

#### Windows Mobile 5.0 for Smartphone

- HTC Faraday, HTC S310, HTC S620, HTC Tornado
- Qtek 8300, Qtek 8310
- Cingular 2125, I-mate SP5, I-mate SP5m Music Smartphone, Samsung SGH-i600, Samsung SGH-i320, T-Mobile MDA II Music, Toshiba Portégé G500

Windows Mobile 6 Professional

HTC P3450 (Touch), HTC Touch Dual, HTC Touch Cruise, HTC TyTN II (Kaiser)

Windows Mobile 6 Standard

HTC S730, HTC S710

## 4 Service Level Agreements

### 4.1 Openingstijden Business Servicedesk

De Business Servicedesk van KPN biedt ondersteuning voor klanten bij eventuele vragen of problemen. De Business Servicedesk is geopend op werkdagen van 08.00 tot 18.00 uur. Op officieel erkende feestdagen is de Business Servicedesk gesloten. KPN erkent de volgende feestdagen: Koninginnedag, 5 mei (éénmaal per vijf jaar), eerste en tweede Paasdag, Hemelvaartsdag, eerste en tweede Pinksterdag, eerste en tweede Kerstdag en Nieuwjaarsdag.

### 4.2 Beschikbaarheid

De dienst Internet Veiligheidspakket wordt 24 uur per dag en 365 dagen per jaar aangeboden. KPN garandeert een minimale beschikbaarheid van 99 procent. KPN streeft ernaar om incidenten en problemen uiterlijk binnen drie werkdagen op te lossen.

De tijd die nodig is om incidenten en problemen op te lossen terwijl de dienstverlening zelf wel beschikbaar blijft, wordt niet meegeteld in de tijd dat de dienst niet beschikbaar is.

Het uitlopen van gepland onderhoud wordt wel meegeteld in de tijd dat de dienst niet beschikbaar is.

Uitgesloten uren worden niet meegeteld in de berekening van de beschikbaarheid. Uitgesloten uren zijn uren waarin de dienstverlening niet beschikbaar is, zonder dat de oorzaak hiervan toe te schrijven is aan KPN. Het kan hierbij onder meer om de volgende storingen gaan:

- Storingen op het internet of het publieke netwerk
- Storingen veroorzaakt door componenten die niet vallen onder de dienstverlening en waarvoor KPN niet verantwoordelijk is
- Storingen veroorzaakt door misbruik van de dienstverlening door u of uw eindgebruikers
- Calamiteiten

### 4.3 Onderhoudsvenster

Gepland onderhoud zal plaatsvinden tijdens het Maintenance Window, op woensdagnacht van 02.00 tot 07.00 uur, (met uitzondering van nationale feestdagen). De tijd dat de dienst niet beschikbaar is door gepland onderhoud neemt maximaal 8 uur per maand in beslag.

## 5 Helpdesk en procedures

### 5.1 Openingstijden Business Servicedesk

Incidenten, problemen en andere zaken kunnen op één van de volgende manieren worden gemeld:

- Per telefoon 0800-0403 (alleen tijdens de openingstijden van de Business Servicedesk van KPN)
- Via website [www.kpn.com/softwareonline](http://www.kpn.com/softwareonline)

### 5.2 Communicatie over onderhoudswerkzaamheden

Als er tijdens gepland onderhoud een wijziging moet worden doorgevoerd die de werking van de dienst beïnvloedt, stelt KPN u ten minste 15 werkdagen van tevoren op de hoogte.

## 6 Tarieven en facturering

### 6.1 Tariefstructuur

KPN brengt voor de dienst Internet Veiligheidspakket een maandelijks tarief in rekening.

### 6.2 Facturering

De dienst Internet Veiligheidspakket wordt elke maand met terugwerkende kracht in rekening gebracht. Betalingen dienen plaats te vinden in euro's en binnen een termijn van 30 dagen.

### 6.3 Contractduur

De standaard contractduur voor het Internet Veiligheidspakket is 1 jaar. Het contract wordt elk jaar automatisch met 1 jaar verlengd. De opzegtermijn is 3 maanden (opzeggen vóór de eerste van de maand). Als u de dienst opwaardeert, wordt uw contract met één jaar verlengd.

U dient de dienst telefonisch op te zeggen via: 0800 0403 optie 4.

## 7 Back-up Online

Gezien de stijgende waarde van digitale informatie, is het maken van back-ups van essentieel belang voor het borgen van de bedrijfsprocessen binnen uw organisatie. Back-up Online van KPN wordt in de meeste gevallen toegepast om ouderwetse, op tape gebaseerde systemen te vervangen. Bijvoorbeeld omdat deze versleten zijn, niet langer voldoende capaciteit bieden, of vanwege de te hoge eigendomskosten, die niet meer bij de hedendaagse bedrijfsvoering passen.

Back-up Online is gebaseerd op een client/server-softwareoplossing waarmee u een back-up kunt maken van de bedrijfskritische gegevens op uw pc of laptop. Wanneer u back-ups wilt maken van gedeelde netwerkstations, kunt u het beste kiezen voor Back-up Online voor Servers.

### 7.1 Voordelen van Back-up Online

Bedrijfskritische informatie op uw pc of laptop die geselecteerd is als onderdeel van de back-up, is altijd verzekerd. Doordat de back-up automatisch wordt uitgevoerd, kunt u nooit een back-up vergeten. Een overzicht ('dashboard') dat u dagelijks per e-mail ontvangt, houdt u op de hoogte van het back-upproces. Als u bestanden kwijtraakt die onderdeel zijn van de back-up, kunt u deze gemakkelijk en snel weer terugplaatsen op uw pc of laptop.

Back-up Online biedt u de volgende voordelen:

- Maximale veiligheid voor uw bedrijfsgegevens
- Altijd een back-up van uw bestanden in een CyberCenter (datacenter) van KPN, dus op een zeer goed beveiligde plaats
- U kunt eenvoudig instellen op welk tijdstip de back-up gemaakt moet worden. Zo vergeet u nooit (meer) om een back-up te maken
- Geen gedoe met tapes of externe harddisks – uw gegevens worden online naar het CyberCenter gestuurd
- U kunt geen tapes of externe harddisks meer kwijtraken

### 7.2 Functies van Back-up Online

De client-software van Back-up Online beschikt standaard over de volgende functies:

- Back-up van bestanden op uw pc of laptop.
- Back-up van geopende bestanden door middel van VSS (Volume Shadow Copy Service)
- Back-up van veel gebruikte mappen:
  - Mijn Favorieten
  - Mijn Documenten
  - Outlook e-mail
  - Outlook Express e-mail

Back-up Online is bereikbaar via bestaande internetverbindingen, zoals ADSL, IP-VPN of IAS.

Met Back-up Online bepaalt u zelf welke gegevens u veilig wilt stellen.

De speciale software zorgt ervoor dat u, na een eenmalige installatie en configuratie, geen omkijken meer heeft naar de automatische back-up. Door middel van het dagelijkse dashboard-bericht van KPN weet u precies welke bestanden zijn veiliggesteld en of er zich eventuele problemen hebben voorgedaan.

### 7.3 Ondersteunde besturingssystemen

De door KPN geleverde back-upsoftware ondersteunt standaard de volgende op Intel gebaseerde besturingssystemen:

- Windows 2000 Workstation
- Windows XP
- Windows Vista

- Mac OS X (10.4 en 10.5, alleen op Intel gebaseerd)

## 7.4 Bewaaropties

Back-up Online biedt de volgende bewaaropties:

- Bestanden waarvan u een back-up heeft gemaakt en die verwijderd zijn van uw pc of laptop worden gedurende de 28 daaropvolgende back-upsessies in ons CyberCenter bewaard
- Bestanden die niet meer bij de back-up zijn inbegrepen, worden gedurende de 28 daaropvolgende back-upsessies bewaard
- Als een bestand dat bij de back-up is inbegrepen iedere dag wordt gewijzigd, dan zijn er van dit bestand maximaal 28 versies beschikbaar

## 7.5 Advisering

KPN kan desgewenst adviezen verstrekken met betrekking tot de strategieën die u kunt toepassen om te bepalen welke bestanden in de back-up moeten worden inbegrepen. KPN kan ook ondersteuning bieden bij de ingebruikname van Back-up Online voor grotere aantallen pc's of laptops in uw organisatie, waardoor u zonder veel voorkennis de applicatie kunt gebruiken.

## 7.6 Beveiligingsaspecten

Aangezien KPN zorgvuldig met uw belangrijkste (vertrouwelijke) gegevens omgaat, is de beveiliging van uw gegevens erg belangrijk. KPN bewaart alle gegevens in twee zeer veilige CyberCenters, op platforms die aan de hoogste standaarden voldoen.

De gegevens worden voor verzending versleuteld volgens de 'AES 128'-standaard (Advanced Encryption Standard). De encryptiesleutel bedenkt u zelf en komt niet op de systemen van KPN te staan. Als u de encryptiesleutel kwijtraakt, kunt u geen bestanden meer herstellen. Alle bestanden worden individueel versleuteld en aldus opgeslagen.

De twee CyberCenters bevinden zich in zeer veilige datacenters (o.a. BS 7799-gecertificeerd):

- Uw belangrijke gegevens worden door drie beveiligingslagen afgeschermd:
  - Gebruikersnaam
  - Wachtwoord
  - Encryptiesleutel (AES 128)
- Ondersteunend personeel van KPN werkt volgens stringente eisen:
  - Versleutelde gegevens zijn niet toegankelijk
  - Er worden strenge procedures gehanteerd bij de afwikkeling van ondersteuningsaanvragen

Jaarlijks worden alle platforms en procedures onderworpen aan een strenge audit door een extern adviesbureau.

## 7.7 Abonnementsvormen

Back-up Online is standaard uitgevoerd met een breed scala aan functies. Alle tarieven die op kpn.com voor de dienst Back-up Online worden genoemd, zijn exclusief uw internettoegang. De abonnementsduur van Back-up Online is één jaar. Het abonnement wordt automatisch met een periode van één jaar verlengd, tot het moment waarop het wordt opgezegd. De dienst moet minimaal drie maanden voor het einde van het desbetreffende jaar schriftelijk worden opgezegd. Het is ook mogelijk om een meerjarig contract aan te gaan.

KPN hanteert een zogeheten 'Fair Use Policy' voor Back-up Online. Deze Fair Use Policy houdt in dat KPN zich, in geval van geconstateerd misbruik of excessief gebruik, het recht voorbehoudt om die maatregelen te treffen die nodig worden geacht om het misbruik of excessief gebruik van Back-up Online tegen te gaan. De door KPN te treffen maatregelen kunnen onder meer (tijdelijke) buitengebruikstelling van Back-up Online inhouden.

Als KPN constateert dat sprake is van gebruik in strijd met de door KPN gehanteerde Fair Use Policy, zal KPN de contractant waarschuwen en deze in de gelegenheid stellen om het gebruik van de dienst

Back-up Online binnen een door KPN gestelde termijn aan te passen. Als de contractant zijn gebruik niet binnen de gestelde termijn aanpast, heeft KPN het recht om zonder verdere waarschuwing de maatregelen te treffen die KPN nodig en passend acht. KPN behoudt zich het recht voor om in extreme gevallen van misbruik of excessief gebruik zonder voorafgaande waarschuwing over te gaan tot het nemen van maatregelen. KPN zal de contractant informeren over de genomen maatregelen.

## 7.8 Bestelwijze

U kunt Back-up Online bestellen via [kpn.com](http://kpn.com); gebruik hiervoor het trefwoord 'Software Online'. Na het invullen van het bestelformulier ontvangt u een orderbevestiging. U ontvangt uw accountgegevens binnen drie werkdagen in een e-mailbericht. Dit e-mailbericht bevat naast uw accountgegevens ook de links waarmee u de software, handleiding en FAQ kunt downloaden.

## 7.9 Beschikbaarheid

Voor de dienst Back-up Online voor pc's wordt ten aanzien van de continue levering de volgende beschikbaarheid gehanteerd:

- 98,5 procent beschikbaarheid (back-up maken en herstellen) op maandbasis, maximaal 10,95 uur per maand niet beschikbaar.
- 99,5 procent beschikbaarheid (back-up maken en herstellen) op jaarbasis, maximaal 43,8 uur per jaar niet beschikbaar.

In het bovenstaande mag het totaal van de niet-beschikbaarheid per maand de jaarnorm niet overschrijden. Gepland onderhoud wordt niet gerekend als niet-beschikbaarheid van de dienst. Daarnaast geldt dat de dienst in principe een technische openstellingstijd heeft van 7 dagen per week, 24 uur per dag, 365 dagen per jaar, met inachtneming van de onderhoudsperiodes.

## 7.10 Uitgangspunten

Voor de dienst Back-up Online voor pc's gelden de volgende uitgangspunten:

- Op de Back-up Online-diensten zijn de Algemene Voorwaarden Software Online van toepassing. Deze voorwaarden kunt u vinden op [kpn.com](http://kpn.com), trefwoord 'Algemene Voorwaarden'
- KPN levert de back-upsoftware waarmee de dienstverlening voor Back-up Online wordt aangeboden
- Er dient rekening te worden gehouden met een IP-koppeling (breedbandverbinding, routerpoorten, firewall-instellingen) tussen uw pc('s) en de Back-up Online-omgeving van KPN
- KPN stelt de back-up capaciteit ter beschikking, maar u blijft zelf verantwoordelijk voor het starten en de inhoud van een back-up
- Facturering vindt plaats door middel van automatische incasso. U ontvangt maandelijks een factuuroverzicht via e-mail
- Ondersteuning wordt alleen geleverd voor de door KPN verstrekte clientsoftware
- KPN levert zowel telefonisch als via de website ondersteuning voor de dienst Back-up Online. Voor uw vragen kunt u naar [www.kpn.com/softwareonline](http://www.kpn.com/softwareonline) gaan. Daarnaast kunt u bellen met de Business Servicedesk van KPN via 0800-0403 (gratis). De Business Servicedesk is op werkdagen geopend van 8.00 tot 20.00 uur en op zaterdag van 10.00 tot 17.00 uur
- KPN levert geen ondersteuning voor andere software en hardware van uw pc of laptop, zoals het besturingssysteem

## 8 CyberCenter

Back-up Online wordt geleverd vanuit een zeer veilig CyberCenter van KPN, dat BS 7799-gecertificeerd is (ISO 17799). Deze certificering houdt in dat het CyberCenter van KPN voldoet aan strenge eisen ten aanzien van de fysieke toegangsbeveiliging, noodstroomvoorziening, klimaatbeheersing, brandbeveiliging en aarding.

### 8.1 Fysieke toegangsbeveiliging

Met de keuze van de locatie van het CyberCenter en de fysieke toegangsbeveiliging worden de risico's van diefstal, brand, inbraak, vandalisme of waterschade zoveel mogelijk beperkt. De CyberCenters van KPN worden 24 uur per dag, 7 dagen per week bewaakt.

### 8.2 Ruimte, lokale bekabeling en stroomvoorziening

De apparatuur en voorzieningen voor de gegevensopslag bevinden zich in een afgesloten ruimte en zijn via snelle verbindingen aangesloten op het KPN-netwerk. Noodstroomvoorzieningen en dieselgeneratoren worden automatisch ingezet als de stroomtoevoer naar het CyberCenter uitvalt.

### 8.3 Aarding en bescherming tegen elektrostatische ontladingen

De hardware voor gegevensopslag is volledig sterageaard. Dit betekent dat alle apparatuur met aparte aardedraden is verbonden met de aardingsstrip. Alle aardingsstrips zijn geaard op het potentiaalvereffeningsnetwerk, dat verbonden is met een aardleiding. Ook alle vloercomponenten zijn afzonderlijk geaard op het potentiaalvereffeningsnetwerk.

### 8.4 Klimaatbeheersing en brandveiligheid

Met een combinatie van verwarming, ventilatie en airconditioning draagt KPN zorg voor een goed geventileerde ruimte met een temperatuur tussen 17 en 23 graden Celsius en een luchtvochtigheid tussen 40 en 60 procent. KPN werkt met valkoeling, waardoor stofophoping tot een minimum wordt beperkt.

Vanzelfsprekend zijn systemen voor brandmelding, brandalarmering en brandbestrijding aanwezig.

## 9 Informatiebeveiliging

### Inleiding

KPN hanteert voor de beveiliging van zijn diensten, organisatie en infrastructuur de internationaal erkende standaard voor informatiebeveiliging ISO 27001 en ISO 27002 als richtlijn. Door het regelmatig (laten) uitvoeren van informatiebeveiligingscontroles, verificatie en in- en externe audits houdt KPN zijn informatiebeveiligingsniveau hoog.

#### 9.1 De ISO 27001 en ISO 27002 richtlijn hoe te implementeren

De ISO 27001 beschrijft hoe een organisatie het managementsysteem voor informatiebeveiliging dient in te richten. In de bijlage van de ISO 27001 worden alle 133 ISO beheersmaatregelen omschreven. In de ISO 27002 worden de praktijkmethoden (best practices) voor implementatie van deze beheersmaatregelen aangegeven.

De 133 beheersmaatregelen zijn verdeeld over de volgende 11 aandachtsgebieden:

1. Beveiligingsbeleid
2. Organisatie van informatiebeveiliging
3. Beheer van bedrijfsmiddelen
4. Beveiliging van personeel
5. Fysieke beveiliging en beveiliging van de omgeving
6. Beheer van communicatie- en bedieningsprocessen
7. Toegangsbeveiliging
8. Verwerving, ontwikkeling en onderhoud van informatiesystemen
9. Beheer van informatiebeveiligingsincidenten
10. Bedrijfscontinuïteitsbeheer
11. Naleving

#### 9.2 Continuïteitsbeheer

KPN beschikt over diverse continuïteitsplannen en over een afdeling crisismanagement. De continuïteitsplannen worden regelmatig geoefend en getest en zijn periodiek onderwerp van een interne/externe audit. Het doel hiervan is risico's te beperken en het borgen van een efficiënt en effectief herstel van onze dienstverlening in geval van een eventuele crisis.

Voor het implementeren van een solide continuïteitsproces hanteert KPN de internationaal erkende standaard BS 25999 als richtlijn.

#### 9.3 Beveiligingsmaatregelen

Maar u kunt zelf ook een belangrijke bijdrage leveren aan het beveiligen van uw informatiestromen en (elektronische) persoonsgegevens. Denk hierbij bijvoorbeeld aan uw gebruikersnaam en wachtwoord of het beveiligen van uw interne draadloze netwerk. Wij adviseren u daarom om zelf ook effectieve beveiligingsmaatregelen te treffen. Dit kan bijvoorbeeld door een erkende installateur in te schakelen.

Voor tips en aanvullende informatie kunt u terecht op onze site:

<http://www.kpn.com/zakelijk/service/veilig-internetten.htm>

Of kijk welke diensten KPN aanbiedt op het gebied van (internet)veiligheid:

<http://www.kpn.com/zakelijk/Meer-diensten.htm>

