Nederlandse norm

# NEN-ISO/IEC 27002

(nl)

Informatietechnologie - Beveiligingstechnieken - Code voor informatiebeveiliging (ISO/IEC 27002:2005,IDT)

Information technology - Security techniques - Code of practice for information security management (ISO/IEC 27002:2005,IDT)

Vervangt NEN-ISO/IEC 17799:2005

ICS 35.040

november 2007

Dit document bevat de vertaling in het Nederlands van de internationale norm ISO/IEC 27002:2005. De internationale norm ISO/IEC 27002:2005 heeft de status van Nederlandse norm.



Normcommissie 381 027 "IT-Beveiligingstechnieken"



NEN

©2007 Nederlands Normalisatie-instituut
Postbus 5059, 2600 GB Delft
Telefoon (015) 2 690 390, Fax (015) 2 690 190

## Inhoud


**Voorwoord** ..... **5**

**0 Inleiding** ..... **6**
0.1 Wat is informatiebeveiliging? ..... 6
0.2 Waarom informatiebeveiliging nodig is ..... 6
0.3 Vaststellen van beveiligingseisen ..... 6
0.4 Inschatten van beveiligingsrisico's ..... 7
0.5 Beheersmaatregelen selecteren ..... 7
0.6 Startpunt voor informatiebeveiliging ..... 7
0.7 Kritische succesfactoren ..... 8
0.8 Het ontwikkelen van bedrijfseigen richtlijnen ..... 9

**1 Onderwerp en toepassingsgebied** ..... **10**

**2 Termen en definities** ..... **10**

**3 Structuur van deze norm** ..... **12**
3.1 Hoofdstukken ..... 12
3.2 Hoofdbeveiligingscategorieën ..... 12

**4 Risicobeoordeling en risicobehandeling** ..... **13**
4.1 Beoordelen van beveiligingsrisico's ..... 13
4.2 Behandelen van beveiligingsrisico's ..... 13

**5 Beveiligingsbeleid** ..... **14**
5.1 Informatiebeveiligingsbeleid ..... 14
5.1.1 Beleidsdocument voor informatiebeveiliging ..... 15
5.1.2 Beoordeling van het informatiebeveiligingsbeleid ..... 15

**6 Organisatie van informatiebeveiliging** ..... **16**
6.1 Interne organisatie ..... 16
6.1.1 Betrokkenheid van de directie bij informatiebeveiliging ..... 17
6.1.2 Coördinatie van informatiebeveiliging ..... 17
6.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging ..... 18
6.1.4 Goedkeuringsproces voor IT-voorzieningen ..... 18
6.1.5 Geheimhoudingsovereenkomst ..... 19
6.1.6 Contact met overheidsinstanties ..... 20
6.1.7 Contact met speciale belangengroepen ..... 20
6.1.8 Onafhankelijke beoordeling van informatiebeveiliging ..... 21
6.2 Externe partijen ..... 22
6.2.1 Identificatie van risico's die betrekking hebben op externe partijen ..... 22
6.2.2 Beveiliging behandelen in de omgang met klanten ..... 23
6.2.3 Beveiliging behandelen in overeenkomsten met een derde partij ..... 25

**7 Beheer van bedrijfsmiddelen** ..... **27**
7.1 Verantwoordelijkheid voor bedrijfsmiddelen ..... 27
7.1.1 Inventarisatie van bedrijfsmiddelen ..... 27
7.1.2 Eigendom van bedrijfsmiddelen ..... 28
7.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen ..... 29
7.2 Classificatie van informatie ..... 29
7.2.1 Richtlijnen voor classificatie ..... 29
7.2.2 Labeling en verwerking van informatie ..... 30

**8 Beveiliging van personeel** ..... **31**
8.1 Voorafgaand aan het dienstverband[)] ..... 31
8.1.1 Rollen en verantwoordelijkheden ..... 31
8.1.2 Screening ..... 32
8.1.3 Arbeidsvoorwaarden ..... 32
8.2 Tijdens het dienstverband ..... 33
8.2.1 Directieverantwoordelijkheid ..... 33
8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging ..... 34

8.2.3 Disciplinaire maatregelen ..... 35
8.3 Beëindiging of wijziging van dienstverband ..... 35
8.3.1 Beëindiging van verantwoordelijkheden ..... 35
8.3.2 Retournering van bedrijfsmiddelen ..... 36
8.3.3 Blokkering van toegangsrechten ..... 36

**9 Fysieke beveiliging en beveiliging van de omgeving ..... 37**
9.1 Beveiligde ruimten ..... 37
9.1.1 Fysieke beveiliging van de omgeving ..... 37
9.1.2 Fysieke toegangsbeveiliging ..... 38
9.1.3 Beveiliging van kantoren, ruimten en faciliteiten ..... 39
9.1.4 Bescherming tegen bedreigingen van buitenaf ..... 39
9.1.5 Werken in beveiligde ruimten ..... 39
9.1.6 Openbare toegang en gebieden voor laden en lossen ..... 40
9.2 Beveiliging van apparatuur ..... 40
9.2.1 Plaatsing en bescherming van apparatuur ..... 40
9.2.2 Nutsvoorzieningen ..... 41
9.2.3 Beveiliging van kabels ..... 42
9.2.4 Onderhoud van apparatuur ..... 42
9.2.5 Beveiliging van apparatuur buiten het terrein ..... 43
9.2.6 Veilig verwijderen of hergebruiken van apparatuur ..... 44
9.2.7 Verwijdering van bedrijfseigendommen ..... 44

**10 Beheer van communicatie- en bedieningsprocessen ..... 44**
10.1 Bedieningsprocedures en verantwoordelijkheden ..... 44
10.1.1 Gedocumenteerde bedieningsprocedures ..... 45
10.1.2 Wijzigingsbeheer ..... 45
10.1.3 Functiescheiding ..... 46
10.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie ..... 46
10.2 Beheer van de dienstverlening door een derde partij ..... 47
10.2.1 Dienstverlening ..... 47
10.2.2 Controle en beoordeling van dienstverlening door een derde partij ..... 48
10.2.3 Beheer van wijzigingen in dienstverlening door een derde partij ..... 48
10.3 Systeemplanning en acceptatie ..... 49
10.3.1 Capaciteitsbeheer ..... 49
10.3.2 Systeemacceptatie ..... 50
10.4 Bescherming tegen virussen en 'mobile code' ..... 50
10.4.1 Maatregelen tegen virussen ..... 51
10.4.2 Maatregelen tegen 'mobile code' ..... 52
10.5 Back-up ..... 52
10.5.1 Reservekopieën maken (back-ups) ..... 52
10.6 Beheer van netwerkbeveiliging ..... 53
10.6.1 Maatregelen voor netwerken ..... 53
10.6.2 Beveiliging van netwerkdiensten ..... 54
10.7 Behandeling van media ..... 55
10.7.1 Beheer van verwijderbare media ..... 55
10.7.2 Verwijdering van media ..... 55
10.7.3 Procedures voor de behandeling van informatie ..... 56
10.7.4 Beveiliging van systeemdocumentatie ..... 57
10.8 Uitwisseling van informatie ..... 57
10.8.1 Beleid en procedures voor informatie-uitwisseling ..... 57
10.8.2 Uitwisselingsovereenkomsten ..... 59
10.8.3 Fysieke media die worden getransporteerd ..... 60
10.8.4 Elektronisch berichtenuitwisseling ..... 60
10.8.5 Systemen voor bedrijfsinformatie ..... 61
10.9 Diensten voor e-commerce ..... 62
10.9.1 E-commerce ..... 62
10.9.2 Onlinetransacties ..... 63
10.9.3 Openbaar beschikbare informatie ..... 64
10.10 Controle ..... 64
10.10.1 Aanmaken audit-logbestanden ..... 65

10.10.2 Controle van systeemgebruik ..... 65
10.10.3 Bescherming van informatie in logbestanden ..... 67
10.10.4 Logbestanden van administrators en operators ..... 67
10.10.5 Registratie van storingen ..... 67
10.10.6 Synchronisatie van systeemklokken ..... 68

**11 Toegangsbeveiliging ..... 68**
11.1 Bedrijfseisen ten aanzien van toegangsbeheersing ..... 68
11.1.1 Toegangsbeleid ..... 69
11.2 Beheer van toegangsrechten van gebruikers ..... 70
11.2.1 Registratie van gebruikers ..... 70
11.2.2 Beheer van speciale bevoegdheden ..... 71
11.2.3 Beheer van gebruikerswachtwoorden ..... 71
11.2.4 Beoordeling van toegangsrechten van gebruikers ..... 72
11.3 Verantwoordelijkheden van gebruikers ..... 73
11.3.1 Gebruik van wachtwoorden ..... 73
11.3.2 Onbeheerde gebruikersapparatuur ..... 74
11.3.3 'Clear desk'- en 'clear screen'-beleid ..... 74
11.4 Toegangsbeheersing voor netwerken ..... 75
11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten ..... 75
11.4.2 Authenticatie van gebruikers bij externe verbindingen ..... 76
11.4.3 Identificatie van netwerkapparatuur ..... 76
11.4.4 Bescherming op afstand van poorten voor diagnose en configuratie ..... 77
11.4.5 Scheiding van netwerken ..... 77
11.4.6 Beheersmaatregelen voor netwerkverbindingen ..... 78
11.4.7 Beheersmaatregelen voor netwerkroutering ..... 78
11.5 Toegangsbeveiliging voor besturingssystemen ..... 79
11.5.1 Beveiligde inlogprocedures ..... 79
11.5.2 Gebruikersindentificatie en -authenticatie ..... 80
11.5.3 Systemen voor wachtwoordbeheer ..... 81
11.5.4 Gebruik van systeemhulpmiddelen ..... 81
11.5.5 Time-out van sessies ..... 82
11.5.6 Beperking van verbindingstijd ..... 82
11.6 Toegangsbeheersing voor toepassingen en informatie ..... 83
11.6.1 Beperken van toegang tot informatie ..... 83
11.6.2 Isoleren van gevoelige systemen ..... 83
11.7 Draagbare computers en telewerken ..... 84
11.7.1 Draagbare computers en communicatievoorzieningen ..... 84
11.7.2 Telewerken ..... 85

**12 Verwerving, ontwikkeling en onderhoud van informatiesystemen ..... 87**
12.1 Beveiligingseisen voor informatiesystemen ..... 87
12.1.1 Analyse en specificatie van beveiligingseisen ..... 87
12.2 Correcte verwerking in toepassingen ..... 88
12.2.1 Validatie van invoergegevens ..... 88
12.2.2 Beheersing van interne gegevensverwerking ..... 89
12.2.3 Integriteit van berichten ..... 89
12.2.4 Validatie van uitvoergegevens ..... 90
12.3 Cryptografische beheersmaatregelen ..... 90
12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen ..... 90
12.3.2 Sleutelbeheer ..... 92
12.4 Beveiliging van systeembestanden ..... 93
12.4.1 Beheersing van operationele programmatuur ..... 93
12.4.2 Bescherming van testdata ..... 94
12.4.3 Toegangsbeheersing voor broncode van programmatuur ..... 95
12.5 Beveiliging bij ontwikkelings- en ondersteuningsprocessen ..... 95
12.5.1 Procedures voor wijzigingsbeheer ..... 96
12.5.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem ..... 97
12.5.3 Restricties op wijzigingen in programmatuurpakketten ..... 97
12.5.4 Uitlekken van informatie ..... 97
12.5.5 Uitbestede ontwikkeling van programmatuur ..... 98

12.6 Beheer van technische kwetsbaarheden ....99
12.6.1 Beheersing van technische kwetsbaarheden ....99

**13 Beheer van informatiebeveiligingsincidenten ....100**
13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken ....100
13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen ....100
13.1.2 Rapportage van zwakke plekken in de beveiliging ....102
13.2 Beheer van informatiebeveiligingsincidenten en -verbeteringen ....102
13.2.1 Verantwoordelijkheden en procedures ....102
13.2.2 Leren van informatiebeveiligingsincidenten ....104
13.2.3 Verzamelen van bewijsmateriaal ....104

**14 Bedrijfscontinuïteitsbeheer ....105**
14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer ....105
14.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer ....105
14.1.2 Bedrijfscontinuïteit en risicobeoordeling ....106
14.1.3 Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging ....107
14.1.4 Kader voor de bedrijfscontinuïteitsplanning ....107
14.1.5 Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen ....108

**15 Naleving ....110**
15.1 Naleving van wettelijke voorschriften ....110
15.1.1 Identificatie van toepasselijke wetgeving ....110
15.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights, IPR) ....110
15.1.3 Bescherming van bedrijfsdocumenten ....111
15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens ....112
15.1.5 Voorkomen van misbruik van IT-voorzieningen ....113
15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen ....113
15.2 Naleving van beveiligingsbeleid en -normen en technische naleving ....114
15.2.1 Naleving van beveiligingsbeleid en -normen ....114
15.2.2 Controle op technische naleving ....114
15.3 Overwegingen bij audits van informatiesystemen ....115
15.3.1 Beheersmaatregelen voor audits van informatiesystemen ....115
15.3.2 Bescherming van hulpmiddelen voor audits van informatiesystemen ....116

**Bibliografie ....117**

**Index ....118**

## Voorwoord

De ISO (International Organization for Standardization) en het IEC (International Electrotechnical Commission) vormen tezamen een stelsel dat gespecialiseerd is in wereldwijde normalisatie. Nationale lichamen die lid zijn van de ISO of het IEC nemen deel aan de ontwikkeling van internationale normen middels technische commissies die door de respectievelijke organisatie werden samengesteld ten behoeve van de normalisatie in specifieke technische werkvelden. Technische commissies van de ISO en het IEC werken samen bij onderwerpen waarin zij een gemeenschappelijk belang hebben. Andere internationale organisaties, zowel overheidsinstanties als NGO's, nemen in samenwerking met de ISO en het IEC ook deel aan deze werkzaamheden. Op het gebied van informatietechnologie hebben de ISO en het IEC een gezamenlijke technische commissie opgericht, ISO/IEC JTC 1.

Internationale normen worden opgesteld overeenkomstig de voorschriften die in de ISO/IEC-richtlijnen deel 2 zijn opgenomen.

De voornaamste taak van de gezamenlijke technische commissie is de voorbereiding van internationale

normen. Ontwerpversies van internationale normen die zijn aangenomen door de gezamenlijke technische commissie, worden ter stemming voorgelegd aan de leden. Publicatie als internationale norm vereist goedkeuring van ten minste 75 % van de stemmen die zijn uitgebracht door deelnemende leden.

Er wordt gewezen op de mogelijkheid dat sommige elementen van dit document onderwerp kunnen zijn van patentrechten. De ISO en het IEC kunnen niet aansprakelijk worden gesteld voor het al dan niet aanduiden van dergelijke patentrechten.

ISO/IEC 27002 werd opgesteld door Joint Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 27, *IT Security techniques.*

Deze eerste editie van ISO/IEC 27002 bevat ISO/IEC 17799:2005 en ISO/IEC 17799:2005/C1:2007. Zijn technische inhoud is identiek aan die van ISO/IEC 17799:2005. ISO/IEC 17799:2005/C1:2007 verandert het nummer van de norm van 17799 in 27002. ISO/IEC 17799:2005 en ISO/IEC 17799:2005/C1:2007 worden voorlopig gehandhaafd tot de tweede editie van ISO/IEC 27002.

# 0 Inleiding

## 0.1 Wat is informatiebeveiliging?

Informatie is een bedrijfsmiddel, dat net als andere belangrijke bedrijfsmiddelen waarde heeft voor een organisatie en voortdurend op een geschikte manier moet zijn beschermd. Dit is vooral belangrijk in het steeds nauwer verweven bedrijfsleven. Door deze toenemende verwevenheid wordt informatie nu blootgesteld aan een toenemend aantal en breder scala bedreigingen en zwakke plekken (zie ook *OECD Guidelines for the Security of Information Systems and Networks*).

Informatie kan in verschillende vormen bestaan. Hij kan zijn afgedrukt of geschreven op papier, elektronisch zijn opgeslagen, per post of via elektronische media worden verzonden, op film worden getoond of mondeling worden uitgewisseld. Informatie behoort altijd op geschikte wijze te worden beschermd, ongeacht de vorm waarin de informatie bestaat of de wijze waarop deze wordt gedeeld of opgeslagen.

Informatiebeveiliging is de bescherming van informatie tegen een breed scala bedreigingen om bedrijfscontinuïteit te waarborgen, bedrijfsrisico's te minimaliseren en investeringsrendementen en bedrijfskansen zo groot mogelijk te maken.

Informatiebeveiliging wordt bereikt door een geschikte verzameling beheersmaatregelen in te zetten, waaronder beleid, werkwijzen, procedures, organisatiestructuren en programmatuur- en apparatuurfuncties. Deze beheersmaatregelen moeten worden vastgesteld, gecontroleerd, beoordeeld en waar nodig verbeterd om te waarborgen dat de specifieke beveiligings- en bedrijfsdoelstellingen van de organisatie worden bereikt. Dit behoort te worden gedaan in samenhang met andere bedrijfsbeheerprocessen.

## 0.2 Waarom informatiebeveiliging nodig is

Informatie en de ondersteunende processen, systemen en netwerken zijn belangrijke bedrijfsmiddelen. Het definiëren, bereiken, onderhouden en verbeteren van informatiebeveiliging kan van essentieel belang zijn voor het behoud van de concurrentiepositie, kasstroom, winstgevendheid, naleving van de wet en het zakelijke imago van de organisatie.

Organisaties en hun informatiesystemen en netwerken worden geconfronteerd met beveiligingsrisico's uit allerlei bronnen, waaronder computerfraude, spionage, sabotage, vandalisme, brand en overstromingen. Oorzaken van schade zoals virussen, computer hacking en 'weigeren-van-dienst'-aanvallen komen steeds vaker voor en worden steeds ambitieuzer en vernuftiger.

Informatiebeveiliging is belangrijk voor ondernemingen en instanties in de publieke en private sector en voor de bescherming van vitale infrastructuur. In beide sectoren zal informatiebeveiliging functioneren als een instrument voor bijvoorbeeld het realiseren van e-government (digitale overheid) of e-business (elektronische handel) en voor het vermijden of verminderen van de inherente risico's. De onderlinge verbondenheid van publieke en private netwerken en het delen van informatiemiddelen maken het steeds moeilijker om de toegang te beheersen. De trend naar gedistribueerde gegevensverwerking heeft de doeltreffendheid van centrale, specialistische beheersing verzwakt.

Veel informatiesystemen zijn niet ontworpen met het oog op veiligheid. De beveiliging die met technische middelen kan worden bereikt is beperkt en behoort te worden ondersteund door geschikt beheer en geschikte procedures. Bepalen welke beheersmaatregelen behoren te worden ingesteld, vereist een zorgvuldige planning en aandacht voor detail. Het beheren van informatiebeveiliging vereist ten minste de inzet van alle werknemers van de organisatie. Bovendien kan deelname van aandeelhouders, leveranciers, derden, klanten of andere externe partijen vereist zijn. Ook kan er specialistisch advies van buiten de organisatie nodig zijn.

## 0.3 Vaststellen van beveiligingseisen

Het is van essentieel belang dat een organisatie haar beveiligingsbehoeften bepaalt. Daarvoor zijn drie hoofdbronnen aan te wijzen.

1) De eerste bron wordt ontleend aan de beoordeling van de risico's voor de organisatie, rekening houdend met de totale bedrijfsstrategie en bedrijfsdoelstellingen van de organisatie. Via risicobeoordeling worden de bedreigingen ten aanzien van bedrijfsmiddelen vastgesteld, worden de kwetsbaarheid voor en waarschijnlijkheid van het optreden van deze bedreigingen beoordeeld en worden de potentiële effecten ervan ingeschat.

2) De tweede bron wordt gevormd door eisen uit wet- en regelgeving en contractuele eisen waaraan de organisatie, haar handelspartners, ingehuurd personeel en dienstverlenende bedrijven moeten voldoen, alsmede hun sociaal-culturele omgeving.

3) De derde bron wordt gevormd door het eigen stelsel van uitgangspunten, doelstellingen en bedrijfseisen voor informatieverwerking dat een organisatie heeft ontwikkeld ter ondersteuning van haar bedrijfsvoering.

## 0.4 Inschatten van beveiligingsrisico's

Beveiligingsbehoeften worden vastgestel aan de hand van methodische beoordeling van beveiligingsrisico's. Uitgaven aan beheersmaatregelen moeten worden afgewogen tegen de bedrijfsschade die zou kunnen ontstaan door beveiligingsincidenten.

De resultaten van deze risicobeoordeling helpen de directie te bepalen welke maatregelen geschikt zijn en welke prioriteiten gelden voor het beheer van de informatiebeveiligingsrisico's en het implementeren van de beheersmaatregelen ter bescherming tegen deze risico's.

De risicobeoordeling behoort regelmatig te worden herhaald om eventuele wijzigingen mee te nemen die van invloed zouden kunnen zijn op de resultaten van de risicobeoordeling.

Nadere informatie over de beoordeling van beveiligingsrisico's is te vinden in 4.1 'Beoordelen van beveiligingsrisico's'.

## 0.5 Beheersmaatregelen selecteren

Zodra de beveiligingsbehoeften en risico's zijn vastgesteld en de besluiten voor de behandeling van de risico's zijn genomen, behoren passende beheersmaatregelen te worden geselecteerd en geïmplementeerd om te waarborgen dat de risico's tot een aanvaardbaar niveau worden verminderd. Beheersmaatregelen kunnen worden geselecteerd uit deze norm of uit andere bronnen, of er kunnen geheel nieuwe beheersmaatregelen worden ontworpen om aan specifieke behoeften te voldoen. De keuze van de beveiligingbeheersmaatregelen is afhankelijk van de besluiten van de organisatie die zijn gebaseerd op de criteria voor risicoacceptatie, risicobehandeling en de algemene aanpak van risicobeheer die in de organisatie wordt toegepast, en behoort ook in lijn te zijn met alle relevante nationale en internationale wet- en regelgeving.

Sommige beheersmaatregelen in deze norm kunnen worden beschouwd als leidraad voor het beheer van informatiebeveiliging en zijn toepasbaar in de meeste organisaties. Ze worden nader uitgelegd onder de kop 'Startpunt voor informatiebeveiliging'.

Nadere informatie over het selecteren van beheersmaatregelen en andere mogelijkheden voor risicobehandeling is te vinden in 4.2. 'Behandelen van beveiligingsrisico's'.

## 0.6 Startpunt voor informatiebeveiliging

Een aantal beheersmaatregelen kan worden beschouwd als een goed uitgangspunt voor het implementeren van informatiebeveiliging. Ze zijn gebaseerd op essentiële wettelijke eisen of ze worden algemeen beschouwd als gebruikelijke praktijk voor informatiebeveiliging.

Tot de beheersmaatregelen die vanuit wettelijk oogpunt van essentieel belang zijn voor een organisatie behoren, afhankelijk van de toepasselijke wetgeving:

a) bescherming van persoonsgegevens (zie 15.1.4);

b) bescherming van specifieke bedrijfsdocumenten (zie 15.1.3);

c) intellectuele eigendomsrechten (zie 15.1.2).

Tot de beheersmaatregelen die worden beschouwd als gebruikelijke praktijk voor informatiebeveiliging behoren:

a) beleidsdocument voor informatiebeveiliging (zie 5.1.1);

b) toewijzen van verantwoordelijkheden voor informatiebeveiliging (zie 6.1.3);

c) bewustmaken van informatiebeveiliging en opleiden en trainen voor (zie 8.2.2);

d) correcte verwerking in toepassingen (zie 12.2);

e) beheer van technische kwetsbaarheid (zie 12.6);

f) beheer van bedrijfscontinuïteit (zie 14);

g) beheer van informatiebeveiligingsincidenten en -verbeteringen (zie 13.2).

Deze beheersmaatregelen gelden voor de meeste organisaties en in de meeste omgevingen.

Er behoort echter op te worden gewezen dat hoewel alle beheersmaatregelen in deze norm belangrijk zijn, de relevantie van een beheersmaatregel altijd behoort te worden vastgesteld in het licht van de specifieke risico's waarmee de organisatie wordt geconfronteerd. Hoewel de bovengenoemde benadering dus wordt beschouwd als een goed uitgangspunt, moet deze niet worden toegepast in plaats van het selecteren van beheersmaatregelen op basis van een risicobeoordeling.

## 0.7 Kritische succesfactoren

De ervaring leert dat de volgende factoren vaak van wezenlijk belang zijn voor een geslaagde implementatie van informatiebeveiliging in een organisatie:

a) informatiebeveiligingsbeleid, doelstellingen en activiteiten die de bedrijfsdoelstellingen weerspiegelen;

b) benadering en kader ten aanzien van het implementeren, onderhouden, controleren en verbeteren van informatiebeveiliging die passen binnen de organisatiecultuur;

c) zichtbare steun en betrokkenheid van alle managementniveaus;

d) goed begrip van informatiebeveiligingseisen, risicobeoordeling en risicobeheer;

e) effectieve marketing van informatiebeveiliging naar alle managers, werknemers en andere partijen om beveiligingsbewustzijn te creëren;

f) verstrekken van richtlijnen over informatiebeveiligingsbeleid en -normen aan alle managers, werknemers en andere partijen;

g) voorzieningen om activiteiten op het gebied van informatiebeveiligingsbeheer te financieren;

h) verzorgen van geschikte training en opleidingen en creëren van beveiligingsbewustzijn;

i) vastleggen van een effectief proces voor beheersing van informatiebeveiligingsincidenten;

j) implementatie van een meetsysteem[1)] om de doeltreffendheid van het beheer van de informatiebeveiliging te beoordelen en suggesties ter verbetering aan te dragen.

## 0.8 Het ontwikkelen van bedrijfseigen richtlijnen

Deze praktijkcode kan worden beschouwd als een uitgangspunt voor het ontwikkelen van richtlijnen die specifiek op de organisatie zijn toegesneden. Mogelijk zijn niet alle beheersmaatregelen en richtlijnen in deze praktijkcode van toepassing. Verder zijn er wellicht aanvullende beheersmaatregelen en richtlijnen nodig die niet in deze norm zijn opgenomen. Wanneer documenten worden ontwikkeld met aanvullende richtlijnen of beheersmaatregelen kan het nuttig zijn te werken met kruisverwijzingen naar hoofdstukken in deze norm waar dat van toepassing is, zodat auditors en handelspartners de naleving kunnen controleren.



1) Informatiebeveiligingsmetingen vallen buiten het toepassingsgebied van deze norm.

# Informatietechnologie – Beveiligingstechnieken – Code voor informatiebeveiliging

## 1 Onderwerp en toepassingsgebied

Deze internationale norm geeft richtlijnen en algemene principes voor het initiëren, implementeren, handhaven en verbeteren van de informatiebeveiliging in een organisatie. De doelstellingen die in deze internationale norm worden beschreven geven generale richtlijnen voor de algemeen aanvaarde doelen van informatiebeveiliging.

De beheersdoelstellingen en beheersmaatregelen van deze internationale norm zijn bedoeld voor implementatie om te voldoen aan de eisen die in een risicobeoordeling zijn vastgesteld. Deze internationale norm kan dienen als een praktische handleiding voor het opstellen van beveiligingsnormen en doeltreffend beheer van informatiebeveiliging voor de organisatie en om te helpen vertrouwen te scheppen in relaties tussen organisaties.

## 2 Termen en definities

Voor de toepassing van dit document gelden de volgende definities.

**2.1**
**bedrijfsmiddel**
alles dat waarde heeft voor de organisatie

[ISO/IEC 13335-1:2004]

**2.2**
**beheersmaatregel**
middel om risico te beheersen, waaronder beleid, procedures, richtlijnen, werkwijzen of organisatiestructuren, die administratief, technisch, beheersmatig of juridisch van aard kunnen zijn

OPMERKING Beheersmaatregel wordt ook gebruikt als een synoniem voor waarborging of tegenmaatregel.

**2.3**
**richtlijn**
beschrijving die verduidelijkt wat behoort te worden gedaan en hoe, om de doelstellingen te bereiken die in het beleid zijn vastgelegd

[ISO/IEC 13335-1:2004]

**2.4**
**IT-voorzieningen**
elk(e) systeem, dienst of infrastructuur voor informatieverwerking, of de fysieke locaties waarin ze zijn ondergebracht

**2.5**
**informatiebeveiliging**
behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie; daarnaast kunnen ook andere eigenschappen, zoals authenticiteit, verantwoording, onweerlegbaarheid en betrouwbaarheid hierbij een rol spelen

**2.6**
**informatiebeveiligingsgebeurtenis**
vastgestelde status van een systeem, dienst of netwerk die duidt op een mogelijke overtreding van het beleid voor informatiebeveiliging of een falen van beveiligingsvoorzieningen, of een tot dan toe onbekende situatie die relevant kan zijn voor beveiliging

[ISO/IEC TR 18044:2004]

**2.7**
**informatiebeveiligingsincident**
afzonderlijke gebeurtenis of een serie ongewenste of onverwachte informatiebeveiligingsgebeurtenissen waarvan het waarschijnlijk is dat ze nadelige gevolgen voor de bedrijfsvoering hebben en een bedreiging vormen voor de informatiebeveiliging

[ISO/IEC TR 18044:2004]

**2.8**
**beleid**
algehele intentie en richting die formeel door de directie wordt onderschreven

**2.9**
**risico**
combinatie van de waarschijnlijkheid van een gebeurtenis en het gevolg ervan

[ISO/IEC Guide 73:2002]

**2.10**
**risicoanalyse**
systematisch gebruik van informatie om bronnen te identificeren en de risico's in te schatten

[ISO/IEC Guide 73:2002]

**2.11**
**risicobeoordeling**
algeheel proces van risicoanalyse en risico-evaluatie

[ISO/IEC Guide 73:2002]

**2.12**
**risico-evaluatie**
proces waarin het ingeschatte risico wordt afgewogen tegen vastgestelde risicocriteria om te bepalen in welke mate het risico significant is

[ISO/IEC Guide 73:2002]

**2.13**
**risicobeheer**
gecoördineerde activiteiten om een organisatie sturing te geven en te bewaken met betrekking tot risico's

OPMERKING Risicobeheer omvat doorgaans risicobeoordeling, risicobehandeling, risicoacceptatie en risicocommunicatie.

[ISO/IEC Guide 73:2002]

**2.14**
**risicobehandeling**
proces van keuze en implementatie van maatregelen om risico's te verlagen

[ISO/IEC Guide 73:2002]

**2.15**
**derde partij**
persoon of entiteit die wat betreft de zaak in kwestie, als onafhankelijk van de betrokken partijen wordt gezien

[ISO/IEC Guide 2:1996]

**2.16**
**bedreiging**
potentiële oorzaak van een ongewenst incident dat een systeem of organisatie schade kan toebrengen

[ISO/IEC 13335-1:2004]

**2.17**
**kwetsbaarheid**
zwakte van een bedrijfsmiddel of groep bedrijfsmiddelen die door een of meer bedreigingen kan worden benut

[ISO/IEC 13335-1:2004]

## 3 Structuur van deze norm

Deze norm bevat 11 hoofdstukken met beveiligingsbeheersmaatregelen, die gezamenlijk 39 hoofdbeveiligingscategorieën omvatten en één inleidend hoofdstuk met een introductie over risicobeoordeling en risicobehandeling.

### 3.1 Hoofdstukken

Elk hoofdstuk omvat een aantal hoofdbeveiligingscategorieën. De elf hoofdstukken (voorzien van het aantal hoofdbeveiligingscategorieën dat in elk hoofdstuk wordt behandeld) zijn:

a) beveiligingsbeleid (1);

b) organisatie van de informatiebeveiliging (2);

c) beheer van bedrijfsmiddelen (2);

d) personele beveiligingseisen (3);

e) fysieke beveiliging en beveiliging van de omgeving (2);

f) beheer van communicatie- en bedieningsprocessen (10);

g) toegangsbeveiliging (7);

h) aanschaf, ontwikkeling en onderhoud van informatiesystemen (6);

i) beheersen van informatiebeveiligingsincidenten (2);

j) beheerproces bedrijfscontinuïteit (1);

k) naleving (3).

OPMERKING De volgorde van de hoofdstukken in deze norm is geen maat van hun belangrijkheid. Afhankelijk van de omstandigheden zouden alle hoofdstukken belangrijk kunnen zijn, daarom behoort iedere organisatie die deze norm toepast, de van toepassing zijnde hoofdstukken te identificeren, vast te stellen hoe belangrijk zij zijn en hoe ze van toepassing zijn voor de afzonderlijke bedrijfsprocessen. Eveneens geven opsommingen en lijsten in deze norm geen volgorde van belangrijkheid aan, tenzij dit wordt vermeld.

### 3.2 Hoofdbeveiligingscategorieën

Elke hoofdbeveiligingscategorie bevat:

— een beheersdoelstelling die vermeldt wat er moet worden bereikt en

— een of meer beheersmaatregelen die kunnen worden toegepast om de beheersdoelstelling te realiseren.

De beschrijving van beheersmaatregelen is als volgt gestructureerd.

Beheersmaatregel
Definieert de specifieke maatregel om aan de beheersdoelstelling te voldoen.

Implementatierichtlijnen
Geven nadere informatie om de implementatie van de beheersmaatregel te ondersteunen en om de beheersdoelstelling te realiseren. Sommige richtlijnen zullen niet in alle gevallen van toepassing zijn; andere manieren om de beheersmaatregel te implementeren kunnen daarom geschikter zijn.

Overige informatie
Verstrekt nadere informatie waarmee rekening moet worden gehouden, bijvoorbeeld juridische overwegingen en verwijzingen naar andere normen.

# 4 Risicobeoordeling en risicobehandeling

## 4.1 Beoordelen van beveiligingsrisco's

Risicobeoordelingen behoren risico's te identificeren en te kwantificeren en prioriteit toe te kennen aan de hand van de criteria voor risicoacceptatie en doelstellingen die relevant zijn voor de organisatie. De resultaten behoren richting te geven bij het bepalen van passende managementactie en -prioriteiten voor het beheersen van informatiebeveiligingsrisico's en voor het implementeren van beheersmaatregelen, genomen om tegen deze risico's te beschermen. Het is mogelijk dat het proces van risicobeoordeling en keuze van beheersmaatregelen een aantal keren moet worden herhaald om de verschillende onderdelen van de organisatie of individuele informatiesystemen af te dekken.

De risicobeoordeling behoort te bestaan uit de systematische aanpak van het schatten van de omvang van de risico's (risicoanalyse) en het vergelijkingsproces van de ingeschatte risico's met risicocriteria om zo het belang van de risico's te bepalen (risico-evaluatie).

Risicobeoordelingen behoren ook periodiek te worden uitgevoerd om in te spelen op wijzigingen in de beveiligingseisen en de risicosituatie, bijv. in de bedrijfsmiddelen, bedreigingen, kwetsbaarheden, invloeden, de risico-evaluatie, en wanneer zich belangrijke wijzigingen voordoen. Deze risicobeoordelingen behoren systematisch te worden uitgevoerd om vergelijkbare en reproduceerbare resultaten te kunnen verkrijgen.

De risicobeoordeling van de informatiebeveiliging behoort, om effectief te zijn, een goed beschreven toepassingsgebied te hebben en behoort, waar van toepassing, relaties te leggen met risicobeoordelingen op andere gebieden.

Het toepassingsgebied van een risicobeoordeling kan zich uitstrekken tot de gehele organisatie, delen van de organisatie, een afzonderlijk informatiesysteem, systeemspecifieke onderdelen of diensten waar dit praktisch, realistisch en handig is. In ISO/IEC TR 13335-3 (*Guidelines for the Management of IT Security – Techniques for the Management of IT Security*) worden voorbeelden van methoden voor risicobeoordeling besproken.

## 4.2 Behandelen van beveiligingsrisico's

De organisatie behoort, alvorens de behandeling van een risico te overwegen, eerst de criteria vast te stellen om te bepalen of risico's al of niet kunnen worden aanvaard. Risico's kunnen bijvoorbeeld worden aanvaard, indien de beoordeling luidt dat het risico laag is of dat de behandelingskosten voor de organisatie niet in verhouding staan tot de opbrengsten. Deze beslissingen behoren te worden vastgelegd.

Voor elk van de risico's vastgesteld na de risicobeoordeling moet een besluit over de risicobehandeling worden genomen. Mogelijke opties voor risicobehandeling zijn:

a) toepassen van gepaste beheersmaatregelen om de risico's te verminderen;

# Bestelformulier

**Stuur naar:**

NEN Standards Products & Services
t.a.v. afdeling Klantenservice
Antwoordnummer 10214
2600 WB Delft


**NEN** Standards Products & Services

Postbus 5059
2600 GB Delft

Vlinderweg 6
2623 AX Delft

T (015) 2 690 390
F (015) 2 690 271

www.nen.nl/normshop


## Ja, ik bestel

__ ex. NEN-ISO/IEC 27002:2007 nl Informatietechnologie - Beveiligingstechnieken - Code voor informatiebeveiliging € 205.65

### Wilt u deze norm in PDF-formaat? Deze bestelt u eenvoudig via www.nen.nl/normshop

**Gratis e-mailnieuwsbrieven**

Wilt u op de hoogte blijven van de laatste ontwikkelingen op het gebied van normen, normalisatie en regelgeving? Neem dan een gratis abonnement op een van onze e-mailnieuwsbrieven. www.nen.nl/nieuwsbrieven

## Gegevens

Bedrijf / Instelling

T.a.v. O M O V

E-mail

Klantnummer NEN

Uw ordernummer BTW nummer

Postbus / Adres

Postcode Plaats

Telefoon Fax

**Factuuradres** (indien dit afwijkt van bovenstaand adres)

Postbus / Adres

Postcode Plaats

Datum Handtekening

**Retourneren**

Fax: 015 2 690 271
E-mail: klantenservice@nen.nl
Post: NEN Standards Products & Services,
t.a.v. afdeling Klantenservice
Antwoordnummer 10214,
2600 WB Delft
(geen postzegel nodig).

**Voorwaarden**

- De prijzen zijn geldig tot 31 december 2018, tenzij anders aangegeven.
- Alle prijzen zijn excl. btw, verzend- en handelingskosten en onder voorbehoud bij o.m. ISO- en IEC-normen.
- Bestelt u via de normshop een pdf, dan betaalt u geen handeling en verzendkosten.
- Meer informatie: telefoon 015 2 690 391, dagelijks van 8.30 tot 17.00 uur.
- Wijzigingen en typefouten in teksten en prijsinformatie voorbehouden.
- U kunt onze algemene voorwaarden terugvinden op: www.nen.nl/leveringsvoorwaarden.