

Verklaring van Toepasseljkheid - De Bouwpas (Versie 1.0 van 17-05-2019)

ISO 27001:2013 Beveiligingsmaatregelen			Maatregel aanwezig?	Reden van aanwezigheid				Geïmplementeerd? (JA/NEE/DEELS)
Clause	Sec	Beheersdoelstellingen en -maatregelen		WR	CO	BR	RA	
Informatie beveiligingsbeleid	5.1	Aansturing door de directie van de informatie beveiliging						
	5.1.1	Beleidsregels voor informatiebeveiliging	ja			x	x	Ja
	5.1.2	Beoordelen van het informatiebeveiligingsbeleid	ja			x	x	Ja
Organiseren van informatie beveiliging	6.1	Interne organisatie						
	6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	ja			x	x	Ja
	6.1.2	Scheiding van taken	ja			x	x	Ja
	6.1.3	Contact met overheidsinstanties	ja			x	x	Ja
	6.1.4	Contact met speciale belangengroepen	ja					Ja
	6.1.5	Informatiebeveiliging in projectbeheer	ja			x	x	Ja
	6.2	Mobiele apparatuur en telewerken						
	6.2.1	Beleid voor mobiele apparatuur	ja			x	x	Ja
	6.2.2	Telewerken	ja			x	x	Ja
	7.1	Voorafgaand aan het dienstverband						
	7.1.1	Screening	ja			x	x	Ja
	7.1.2	Arbeidsvoorwaarden	ja	x		x	x	Ja
	7.2	Tijdens het dienstverband						

Verklaring van toepasseljkheid

Veilig personeel	7.2.1	Directieverantwoordelijkheden	ja			x	x	Ja
	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	ja			x	x	Ja
	7.2.3	Disciplinaire procedure	ja			x	x	Ja
	7.3	Beeindiging en wijziging van dienstverband						
	7.3.1	Beeindiging en wijziging van verantwoordelijkheden van het dienstverband	ja	x		x	x	Ja
Beheer van bedrijfsmiddelen	8.1	Verantwoordelijkheid voor bedrijfsmiddelen						
	8.1.1	Inventariseren van bedrijfsmiddelen	ja			x	x	Ja
	8.1.2	Eigendom van bedrijfsmiddelen	ja			x	x	Ja
	8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	ja			x	x	Ja
	8.1.4	Teruggeven van bedrijfsmiddelen	ja			x	x	Ja
	8.2	Informatieclassificatie						
	8.2.1	Classificatie van informatie	ja				x	Ja
	8.2.2	Informatie labelen	ja				x	Ja
	8.2.3	Behandelen van bedrijfsmiddelen	ja			x	x	Ja
	8.3	Behandelen van media						
	8.3.1	Beheer van verwijderbare media	ja			x	x	Ja
	8.3.2	Verwijderen van media	ja			x	x	Ja
	8.3.3	Media fysiek overdragen	ja		x	x	x	Ja
	9.1	Bedrijfseisen voor toegangsbeveiliging						
	9.1.1	Beleid voor toegangsbeveiliging	ja			x	x	Ja

Verklaring van toepasseljkheid

Toegangsbeveiliging	9.1.2	Toegang tot netwerken en netwerkdiensten	ja			x	x	Ja
	9.2	Beheer van toegangsrechten van gebruikers						
	9.2.1	Registratie en uitschrijving van gebruikers	ja			x	x	Ja
	9.2.2	Gebruikers toegang verlenen	ja			x	x	Ja
	9.2.3	Beheren van speciale toegangsrechten	ja			x	x	Ja
	9.2.4	Beheer van geheime authenticatie informatie van gebruikers	ja			x	x	Ja
	9.2.5	Beoordeling van toegangsrechten van gebruikers	ja			x	x	Ja
	9.2.6	Toegangsrechten intrekken of aanpassen	ja			x	x	Ja
	9.3	Gebruikersverantwoordelijkheden						
	9.3.1	Geheime authenticatie gebruiken	ja			x	x	Ja
	9.4	Toegangsbeveiliging van systeem en toepassing						
	9.4.1	Beperking toegang tot informatie	ja			x	x	Ja
	9.4.2	Beveiligde inlogprocedures	ja			x	x	Ja
	9.4.3	Systeem voor wachtwoordbeheer	ja			x	x	Ja
	9.4.4	Speciale systeemhulpmiddelen gebruiker	ja			x		Ja
9.4.5	Toegangsbeveiliging op programmabroncode	ja			x	x	Ja	
Cryptografie	10.1	Cryptografische beheersmaatregelen						
	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	ja			x	x	Ja
	10.1.2	Sleutelbeheer (cryptografisch)	ja			x	x	Ja

Verklaring van toepasselijkheid

Fysieke beveiliging en beveiliging van de omgeving	11.1	Beveiligde gebieden						
	11.1.1	Fysieke beveiligingszone	ja			x	x	Ja
	11.1.2	Fysieke toegangsbeveiliging	ja			x	x	Ja
	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	ja			x	x	Ja
	11.1.4	Beschermen tegen bedreigingen van buitenaf	ja			x	x	Ja
	11.1.5	Werken in beveiligde gebieden	ja			x	x	Ja
	11.1.6	Laad- en loslocatie	ja			x	x	Ja
	11.2	Apparatuur						
	11.2.1	Plaatsing en bescherming van apparatuur	ja			x	x	Ja
	11.2.2	Nutsvoorzieningen	ja			x	x	Ja
	11.2.3	Beveiliging van bekabeling	ja			x	x	Ja
	11.2.4	Onderhoud van apparatuur	ja			x	x	Ja
	11.2.5	Verwijdering van bedrijfsmiddelen	ja			x		Ja
	11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	ja			x		Ja
	11.2.7	Veilig verwijderen of hergebruiken van apparatuur	ja			x	x	Ja
11.2.8	Onbeheerde gebruikersapparatuur	ja			x	x	Ja	
11.2.9	Clear Desk and Clear Screen beleid	ja			x	x	Ja	
	12.1	Bedieningsprocedures en verantwoordelijkheden						
	12.1.1	Gedocumenteerde bedieningsprocedures	ja			x	x	Ja
	12.1.2	Wijzigingsbeheer	ja			x	x	Ja

Verklaring van toepasselijkheid

Beveiliging bedrijfsvoering	12.1.3	Capaciteitsbeheer	ja			x	x	Ja
	12.1.4	Scheiding van ontwikkel-, test- en productie omgevingen	ja			x	x	Ja
	12.2	Bescherming tegen malware						
	12.2.1	Beheersmaatregelen tegen malware	ja			x	x	Ja
	12.3	Back-up						
	12.3.1	Back-up van informatie	ja			x	x	Ja
	12.4	Verslaglegging en monitoren						
	12.4.1	Gebeurtenissen registreren	ja			x	x	Ja
	12.4.2	Beschermen van informatie in logbestanden	ja			x	x	Ja
	12.4.3	Logbestanden van beheerders en operators	ja			x	x	Ja
	12.4.4	Kloksynchronisatie	ja			x	x	Ja
	12.5	Beheersing van operationele software						
	12.5.1	Software installeren op operationele systemen	ja			x	x	Ja
	12.6	Beheer van technische kwetsbaarheden						
	12.6.1	Beheer van technische kwetsbaarheden	ja			x	x	Ja
	12.6.2	Beperkingen voor het installeren van software	ja			x	x	Ja
	12.7	Overwegingen betreffende audits op informatiesystemen						
	12.7.1	Beheersmaatregelen betreffende audits op informatiesystemen	ja			x	x	Ja
	13.1	Beheer van netwerkbeveiliging						
	13.1.1	Beheersmaatregelen voor netwerken	ja			x	x	Ja

Verklaring van toepasseljkheid

**Communicatie
beveiliging**

13.1.2	Beveiliging van netwerkdiensten	ja			x	x	Ja
13.1.3	Scheiding in netwerken	ja			x	x	Ja
13.2	Informatietransport						
13.2.1	Beleid en procedures voor informatie transport	ja			x	x	Ja
13.2.2	Overeenkomsten over informatie transport	ja			x	x	Ja
13.2.3	Elektronische berichten	ja			x	x	Ja
13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	ja		x	x	x	Ja

**Acquisitie, ontwikkeling
en onderhoud van
informatiesystemen**

14.1	Beveiligingseisen voor informatiesystemen						
14.1.1	Analyse en specificatie van informatiebeveiligingseisen	ja			x	x	Ja
14.1.2	Toepassingsdiensten op openbare netwerken beveiligen	ja			x	x	Ja
14.1.3	Transacties van toepassingsdiensten beschermen	ja			x	x	Ja
14.2	Beveiliging in ontwikkelings- en ondersteunende processen						
14.2.1	Beleid voor beveiligd ontwikkelen	ja			x	x	Ja
14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	ja			x	x	Ja
14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	ja			x	x	Ja
14.2.4	Beperkingen op wijzigingen aan softwarepakketten	ja			x	x	Ja
14.2.5	Principes voor engineering van beveiligde systemen	ja			x	x	Ja
14.2.6	Beveiligde ontwikkelomgeving	ja			x	x	Ja

Verklaring van toepasseljkheid

14.2.7	Uitbestede software ontwikkeling	ja			x	x	Ja
14.2.8	Testen van systeem beveiliging	ja			x	x	Ja
14.2.9	Systeemacceptatietests	ja			x	x	Ja
14.3	Testgegevens						
14.3.1	Bescherming van testgegevens	ja			x	x	Ja

Leveranciersrelaties	15.1	Informatiebeveiliging in leveranciersrelaties						
	15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties	ja			x	x	Ja
	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	ja			x	x	Ja
	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	ja			x	x	Ja
	15.2	Beheer van dienstverlening van leveranciers						
	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	ja			x	x	Ja
	15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	ja			x	x	Ja

Beheer van informatie beveiligingsincidenten	16.1	Beheer van informatiebeveiligingsincidenten en -verbeteringen						
	16.1.1	Verantwoordelijkheden en procedures	ja	x	x	x	x	Ja
	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	ja	x	x		x	Ja
	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	ja		x	x	x	Ja
	16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	ja	x	x		x	Ja

Verklaring van toepasselijkheid

	16.1.5	Respons op informatiebeveiligingsincidenten	ja	x	x		x	Ja
	16.1.6	Lering uit informatiebeveiligingsincidenten	ja			x	x	Ja
	16.1.7	Verzamelen van bewijsmateriaal	ja	x	x		x	Ja
Informatiebeveiligings- aspecten van bedrijfscontinuïteit	17.1	Informatiebeveiligingscontinuïteit						
	17.1.1	Informatiebeveiligingscontinuïteit plannen	ja			x	x	Ja
	17.1.2	Informatiebeveiligingscontinuïteit implementeren	ja			x	x	Ja
	17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	ja			x	x	Ja
	17.2	Redundante componenten						
	17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	ja			x	x	Ja
Naleving	18.1	Naleving van wettelijke en contractuele eisen						
	18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	ja	x		x	x	Ja
	18.1.2	Intellectuele eigendomsrechten	ja	x		x	x	Ja
	18.1.3	Beschermen van registraties	ja	x			x	Ja
	18.1.4	Privacy en bescherming van persoonsgegevens	ja	x			x	Ja
	18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	ja	x			x	Ja
	18.2	Informatiebeveiligingsbeoordelingen						

Verklaring van toepasselijkheid

18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	ja	x			x	Ja
18.2.2	Naleving van beveiligingsbeleid en -normen	ja	x			x	Ja
18.2.3	Beoordeling van technische naleving	ja	x			x	Ja

Legenda (voor geselecteerde maatregelen en redenen voor selectie)

WR: Wet- en regelgeving, **CO:** contractuele overeenkomst, **BR/BP:** business requirements / adopted best practices, **RRA:** resultaat risico assessment,