centrum voor criminaliteitspreventie en veiligheid

Churchilllaan 11
3527 GV Utrecht
Postbus 14069
3508 SC Utrecht

T (030) 751 67 00
F (030) 751 67 01
I www.hetccv.nl

CCV-reglement Kwaliteitslogo

ARTIKEL 1 ALGEMEEN

In dit reglement worden de volgende begrippen gebruikt:

CCV	Centrum voor Criminaliteitspreventie en Veiligheid in Utrecht
CCV-kwaliteitsregeling	Een set eisen en regels van het CCV voor certificatie of inspectie, vastgelegd in een certificatieschema of inspectieschema
Merk	Het CCV-kwaliteitslogo
Licentienemer	De certificatie-instelling of inspectie-instelling die een geldige licentieovereenkomst met het CCV heeft
Certificaathouder	• Leverancier van een product of dienst die een certificaat heeft ontvangen van een certificatie-instelling • Een organisatie die voor hun kwaliteitsmanagementsysteem een certificaat heeft ontvangen van een certificatie-instelling • Een organisatie die een inspectiecertificaat heeft ontvangen van een inspectie-instelling

ARTIKEL 2 TOEPASSELIJKHEID

2.1. Dit reglement geldt voor het gebruik van het CCV-kwaliteitslogo (merk).

2.2. Het merk bestaat uit het volgende beeldmerk:

2.3. Het merk geeft aan dat een gecertificeerd product, gecertificeerde dienst, gecertificeerd kwaliteitsmanagementsysteem of een inspectie voldoet aan de eisen van een CCV-kwaliteitsregeling. Bijlage A van dit reglement bevat een overzicht van de CCV-kwaliteitsregelingen waarvoor het merk wordt toegepast.

2.4. Het merk is eigendom van het CCV.

2.5. Het CCV geeft het gebruik van het merk in licentie aan licentienemers op basis van de CCV-kwaliteitsregeling waarvoor het merk toegepast wordt.

2.6. Aanpassing van het merk of delen hiervan is niet toegestaan, tenzij het CCV daarvoor schriftelijke toestemming geeft.

ARTIKEL 3 RECHTEN EN PLICHTEN

3.1. Licentienemers gebruiken het merk volgens dit reglement.

3.2. Licentienemers kunnen een sublicentie verstrekken aan certificaathouders. Certificaathouders mogen het merk gebruiken zolang hun contract met de licentienemer geldig is. Schorsing van het contract houdt tevens schorsing van het gebruik van het merk in.

3.3. Elk ander gebruik van het merk is niet toegestaan, tenzij het CCV daarvoor schriftelijke toestemming geeft.

3.4. Certificaathouders mogen het gebruik van het merk niet aan derden overdragen.

3.5. Licentienemers leggen in het contract met certificaathouders vast dat dit reglement bindend is.

3.6. Licentienemers registreren de sublicenties en verstrekken hierover op verzoek informatie aan het CCV.

3.7. Certificaathouders registreren waar het merk wordt gebruikt en verstrekken hierover op verzoek informatie aan de licentienemer of het CCV.

3.8. Het recht van de certificaathouder om het merk te gebruiken vervalt direct bij beëindiging van het contract met de licentienemer.

3.9. Het recht van de licentienemer om het merk te verlenen vervalt direct bij beëindiging van de licentieovereenkomst met het CCV.

ARTIKEL 4 GEBRUIK VAN HET MERK

4.1. Het merk wordt alleen gebruikt in directe relatie met de bijbehorende CCV-kwaliteitsregeling. Als de CCV-kwaliteitsregeling nadere bepalingen over het gebruik van het merk bevat, dan zijn deze naast dit reglement onverkort van toepassing.
4.2. Het merk mag worden toegepast als volledig aan de eisen in de CCV-kwaliteitsregeling is voldaan.
4.3. De vorm, grootte, typografische uitvoering en kleur van het merk voldoen aan de voorschriften in bijlage B van dit reglement.
4.4. Gebruik van het merk in publicaties, e-mail, websites, briefpapier en vergelijkbare uitingen is enkel toegestaan met een verwijzing naar de activiteiten van de bijbehorende CCV-kwaliteitsregeling.
4.5. Het merk mag niet worden gebruikt als eigen merk, fabrieksmerk of handelsmerk.

ARTIKEL 5 MERKMISBRUIK

5.1. De licentienemer houdt toezicht op correct gebruik van het merk.
5.2. Bij misbruik van het merk door een certificaathouder, legt de licentienemer sancties op zoals beschreven in de CCV-kwaliteitsregeling.
5.3. De licentienemer is verplicht om merkmisbruik door derden te melden bij het CCV.
5.4. Het CCV kan optreden bij merkmisbruik door andere partijen dan licentienemers of certificaathouders en hen sancties opleggen zoals beschreven in artikel 6.
5.5. Het CCV is niet aansprakelijk voor de consequenties van merkmisbruik.

ARTIKEL 6 MAATREGELEN

6.1. Bij misbruik van het merk door niet-licentienemers of niet-certificaathouders neemt het CCV de volgende maatregelen:
   a. Het geven van een waarschuwing;
   b. Het opleggen van een nader te bepalen boete;
   c. Het opleggen van de verplichting om het CCV te informeren over de omvang van het merkmisbruik;
   d. Het opleggen van de verplichting de partijen als bedoeld onder c. te informeren over het merkmisbruik;
   e. Publicatie in één of meerdere dagbladen, periodieken en/of op websites met vermelding van de naam van de organisatie of persoon en met vermelding van de aard van het merkmisbruik;
   f. Het informeren van de andere partijen over het merkmisbruik en/of neerleggen van een klacht over het merkmisbruik bij een hogere instantie
6.2. Kosten die aan deze maatregelen zijn verbonden, komen voor rekening van de overtreder.

ARTIKEL 7 SLOTBEPALINGEN

7.1. Het CCV is bevoegd dit reglement aan te passen, met inachtneming van een passende overgangstermijn indien de wijziging dit noodzakelijk maakt.
7.2. Dit reglement gaat in op 15 mei 2025.

BIJLAGE A: OVERZICHT VAN DE CCV-KWALITEITSREGELINGEN WAARVOOR HET MERK WORDT TOEGEPAST

A.1 Kwaliteitsregelingenoverzicht

CCV-KWALITEITSREGELING	ONDERWERP VAN CONFORMITEIT	SPECIFICATIE VAN DE EISEN IN
BORG-A	Beveiligingsplan tegen inbraak	Hoofdstuk 2 van de kwaliteitsregeling
BORG-B	Bouwkundige beveiligingsmaatregelen tegen inbraak	Hoofdstuk 2 van de kwaliteitsregeling
BORG-E	Elektronische beveiligingsmaatregelen tegen inbraak	Hoofdstuk 2 van de kwaliteitsregeling
Cyber Security Awareness Training	Proces van aanbieden, uitvoeren en evalueren van cyber security awaress trainingen	Hoofdstuk 2 van de kwaliteitsregeling, ISO 9001 en ISO 27001
Cyber Security Pen Test	Uitvoering en rapportage van penetratietesten	Hoofdstuk 2 van de kwaliteitsregeling
Cyber Security CYRA-IT	Cyberweerbaarheid van (het onderdeel van) de organisatie	Toetsingskader CYRA volgens onderstaande specificaties A2 tot en met A5, die gebaseerd zijn op hoofdstuk 2, bijlage B en C van de kwaliteitsregeling en ISO/IEC 27001 en ISO/IEC 27701
Cyber Security CYRA-NDO	Weerbaarheid van (het onderdeel van) de organisatie tegen digitale ondermijning	Toetsingskader CYRA-NDO volgens onderstaande specificaties A2 en A.6, die gebaseerd zijn op hoofdstuk 2, bijlage B en C van de kwaliteitsregeling, ISO/IEC 27001, ISO/IEC 27701 en Normenkader NDO
Uitgangspuntendocument Brandbeveiliging	Ontwerpeisen aan een brandbeveiligingssysteem	Hoofdstuk 2 van de kwaliteitsregeling
Woningsprinklerinstallaties	Woningsprinklerinstallaties	Hoofdstuk 2 van de kwaliteitsregeling

Specificatie van de eisen voor het keurmerk CYRA-IT:

A.2 Inhoudsopgave Toetsingskader CYRA niveau Entry

ENTRY	NORMELEMENT UIT ISO 27001
A.2.1. Organisatie	
■ Beleidsregels voor informatiebeveiliging en privacy	5.1
■ Toegangsbeveiliging	5.15
■ Registratie en uitschrijving van gebruikers	5,16
■ Toegangsrechten	5.18
■ Rollen en verantwoordelijkheden bij informatiebeveiliging en privacy	5.2
■ Monitoring van, beoordeling van en beheer van veranderingen in de dienstverlening van leveranciers	5.22
■ Informatiebeveiliging in ongunstige situaties	5.29
A.2.2. Personeel	
■ Screening	6.1
■ Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	6.3
■ Telewerken	6.7
■ Rapportage van informatiebeveiligingsgebeurtenissen	6.8
A.2.3. Fysiek	
■ Fysieke beveiligingszone	7.1
A.2.4. Technologisch	
■ Genereren, bewaren en beoordelen van logbestanden	8.15
■ Beschermen van informatie in netwerken en ondersteunende systemen	8.20
■ Veiligheid in het gebruik van netwerkdiensten garanderen.	8.21
■ Garanderen van goed en effectief gebruik van versleuteling om vertrouwelijkheid, integriteit en beschikbaarheid te garanderen in lijn met van toepassing zijnde wet- en regelgeving.	8.24
■ Beleid voor beveiligd ontwikkelen van software en systemen	8.25
■ Informatiebeveiligingseisen in ontwerp en aanschaf van applicaties.	8.26
■ Wijzigingsbeheer	8.32
■ Beveiligde inlogprocedures.	8.5
■ Technische en organisatorische bescherming tegen malware	8.7

■ Voorkomen van exploitatie van technische kwetsbaarheden	8.8
	Paragraaf uit ISO 27701
A.2.5. Privacy	
■ Doeleinden van de organisatie	B.8.2.2
■ Registraties met betrekking tot het verwerken van persoonsgegevens	B.8.2.6

A.3 Inhoudsopgave Toetsingskader CYRA niveau Basic

BASIC NIVEAU BASIC BEVAT ALLE BEHEERSMAATREGELEN VAN HET NIVEAU **ENTRY**, AANGEVULD MET	**NORMELEMENT UIT ISO 27001**
A.3.1. Organisatie	
■ Classificatie van informatie	5.12
■ Informatiebeveiligingsbeleid voor leveranciersrelaties	5.19
■ Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	5.20
■ Toeleveringsketen van informatie- en communicatietechnologie	5.21
■ Informatiebeveiliging voor het gebruik van clouddiensten	5.23
■ Lering uit informatiebeveiligingsincidenten	5.27
■ Privacy en bescherming van persoonsgegevens	5.34
■ Gedocumenteerde bedieningsprocedures	5.37
■ Informatie en analyse over dreigingen	5.7
■ Inventarisatie van informatie en andere samenhangende bedrijfsmiddelen	5.9
A.3.2. Personeel	
■ Arbeidsvoorwaarden	6.2
■ Vertrouwelijkheids- of geheimhoudingsovereenkomst	6.6
A.3.3. Fysiek	
■ Beveiliging van bekabeling	7.12
■ Veilig verwijderen of hergebruiken van apparatuur	7.14
■ Fysieke toegangsbeveiliging	7.2
■ Kantoren, ruimten en faciliteiten beveiligen	7.3
■ Monitoren van de fysieke beveiliging	7.4
■ Beschermen tegen bedreigingen van buitenaf	7.5
■ Werken in beveiligde gebieden	7.6

■ ‘Clear desk’- en ‘clear screen’-beleid	7.7
■ Plaatsing en bescherming van apparatuur	7.8
■ Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	7.9
A.3.4. Technologisch	
■ Beheersing van informatie die wordt opgeslagen of verwerkt op werkplekken en/of mobiele apparaten.	8.1
■ Wissen van informatie	8.10
■ Voorkomen van gegevenslekken	8.12
■ Back-up van informatie	8.13
■ Beschermen van operationele systemen door procedures en maatregelen voor de installatie van software	8.19
■ Beheren van speciale toegangsrechten	8.2
■ Beperking toegang tot informatie	8.3
	Paragraaf uit ISO 27701
A.3.5. Privacy	
■ Overeenkomst met de klant	B.8.2.1
■ Bekendmaking van onderaannemers die worden ingezet voor het verwerken van persoonsgegevens	B.8.5.6
■ Verplichtingen van klanten	B.8.2.5

A.4 Inhoudsopgave Toetsingskader CYRA niveau Intermediate

INTERMEDIATE NIVEAU INTERMEDIATE BEVAT ALLE BEHEERSMAATREGELEN VAN DE NIVEAUS **ENTRY** EN **BASIC**, AANGEVULD MET:	**NORMELEMENT UIT ISO 27001**
A.4.1. Organisatie	
■ Aanvaardbaar gebruik van informatie en overige bedrijfsmiddelen	5.10
■ Teruggeven van bedrijfsmiddelen	5.11
■ Informatie labelen	5.13
■ Authenticatie-informatie	5.17
■ Verantwoordelijkheden en procedures	5.24
■ Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	5.25
■ Respons op informatiebeveiligingsincidenten	5.26
■ Scheiding van taken	5.3

■ Vaststellen van toepasselijke wetgeving en contractuele eisen	5.31
■ Intellectuele eigendomsrechten	5.32
■ Beschermen van registraties	5.33
■ Naleving van beveiligingsbeleid/-normen	5.36
■ Directieverantwoordelijkheden	5.4
■ Informatiebeveiliging in projectbeheer	5.8
A.4.2. Personeel	
■ Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	6.5
A.4.3. Fysiek	
■ Opslagmedia	7.10
■ Nutsvoorzieningen	7.11
■ Onderhoud van apparatuur	7.13
A.4.4. Technologisch	
■ Beschikbaarheid van informatie-verwerkende faciliteiten	8.14
■ Monitoren van activiteiten	8.16
■ Kloksynchronisatie	8.17
■ Scheiding in netwerken	8.22
■ Testen van beveiliging tijdens ontwikkeling en acceptatie	8.29
■ Uitbestede softwareontwikkeling	8.30
■ Capaciteitsbeheer	8.6
	Paragraaf uit ISO 27701
A.4.5. Privacy	
■ Opdracht die inbreuk oplevert	B.8.2.4
■ Retournering, doorgifte of verwijdering van persoonsgegevens	B.8.4.2
■ Registraties van de verstrekking van persoonsgegevens aan derden	B.8.5.3

A.5 Inhoudsopgave Toetsingskader CYRA niveau Advanced

ADVANCED NIVEAU ADVANCED BEVAT ALLE BEHEERSMAATREGELEN VAN DE NIVEAUS **ENTRY, BASIC** EN **INTERMEDIATE**, AANGEVULD MET	**NORMELEMENT ISO 27001**
A.5.1. Organisatie	

VEILIGHEID
MAKEN
WE SAMEN

■ Informatietransport	5.14
■ Verzamelen van bewijsmateriaal	5.28
■ ICT-gereedheid voor bedrijfscontinuïteit	5.30
■ Onafhankelijke beoordeling van informatiebeveiliging	5.35
■ Contact met overheidsinstanties	5.5
■ Contact met speciale belangengroepen	5.6
A.5.2. Personeel	
■ Disciplinaire procedure	6.4
A.5.3. Technologisch	
■ Maskeren van gegevens	8.11
■ Speciale systeemhulpmiddelen gebruiken	8.18
■ Toepassen van web-filters	8.23
■ Principes voor engineering van beveiligde systemen	8.27
■ Veilig coderen	8.28
■ Scheiding van ontwikkel-, test- en productieomgevingen	8.31
■ Bescherming van testgegevens	8.33
■ Beheersmaatregelen betreffende audits van informatiesystemen	8.34
■ Toegangsbeveiliging op programmabroncode	8.4
■ Configuratiebeheer	8.9

A.6 Inhoudsopgave Normkader Digitale Ondermijning

NORMKADER DIGITALE ONDERMIJNING BEOORDELING VAN HET NORMKADER DIGITALE ONDERMIJNING VINDT PLAATS IN COMBINATIE MET BEOORDELING VAN DE BEHEERSMAATREGELEN VOOR HET NIVEAU **ENTRY** UIT HET TOETSINGKADER CYRA	**NORMELEMENT ISO 27001**
■ Beleidsregels voor informatiebeveiliging en privacy **Heeft de organisatie actuele beleidsregels omtrent informatiebeveiliging en privacy?**	5.1
■ Informatie en analyse over dreigingen **Wordt er gekeken naar bedreigingen op het gebied van informatiebeveiliging?**	5.7
■ Inventarisatie van informatie en andere samenhangende bedrijfsmiddelen **Worden de met informatie samenhangende bedrijfsmiddelen vastgelegd?**	5.9
■ Classificatie van informatie **Hanteert de organisatie een classificatiemechanisme?**	5.12

■ Screening **Wordt de achtergrond van personeel geverifieerd?**	n.v.t., aanvullend aspect NDO 1
■ Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging **Wordt kennis van het personeel op peil gebracht/gehouden?**	6.3
■ Meldpunt ondermijning **Wordt gebruik gemaakt van een ondermijningsmeldpunt?**	n.v.t., aanvullend aspect NDO 2
■ 'User endpoint devices' **Wordt gebruikersapparatuur (laptop, PC, tablet, smartphone) dat als onderdeel van de werkplek fungeert beschermd?**	8.1
■ Genereren, bewaren en beoordelen van logbestanden **Wordt er gebruik gemaakt van logbestanden?**	8.15

BIJLAGE B: INSTRUCTIES

Het CCV beheert digitale versies van het merk. Het CCV stelt deze ter beschikking aan licentienemers. Certificatie-instellingen stellen het merk ter beschikking aan certificaathouders.

Het beeldmerk moet zoveel mogelijk op witte en lichtgekleurde ondergronden worden gebruikt. Bij gebruik op gekleurde ondergronden wordt een witte rand om het logo zichtbaar. Deze moet intact blijven.

Aan het beeldmerk is één kleur gekoppeld: PANTONE Process Blue.

- CMYK kleurstelling: C100, M10, Y0, K5.
- RGB kleurstelling: R0, G144, B211.
- Transparante snijfolie Aslan 11381.
- Dekkende folie Avery 809.

Voor spuit- en verfwerk is geen RAL-kleur beschikbaar, maar deze kan op bestelling wel gemengd worden.

Onder het beeldmerk wordt altijd, in grijze en blauwe tekst, het toepassingsgebied van het beeldmerk vermeld. Voor de kleur blauw gelden dezelfde kleurcodes als hierboven vermeld. Voor de kleur grijs gelden onderstaande kleurcodes.

- CMYK kleurstelling: C0, M0, Y0, K60.
- RGB kleurstelling: R:135, G135, B135.