Instituut
Fysieke
Veiligheid

Beleidskader Toegangsbeveiliging

Versie: 1.0, 21 oktober 2014

Instituut Fysieke Veiligheid
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.ifv.nl
info@ifv.nl
026 355 24 00

Documenthistorie

Datum	Versie	Beschrijving	Auteur
09-05-2014	0.1	Eerste opzet	Emiel Wojcik
14-05-2014	0.2	Aanpassingen na review Mark en Alexander	Emiel Wojcik
24-07-2014	0.3	Aanpassingen na reactie netwerken	Emiel Wojcik
21-10-2014	1.0	Definitief gemaakt na vaststelling door regiegroep	Emiel Wojcik

Distributie

Naam	0.1	0.2	0.3	1.0					
Alexander Bouman	X	X							
Mark Aukema	X	X	X						
Netwerk Functioneel Beheer		X	X						
Mounir Bouzed		X	X						
Tae Gaasbeek		X	X						
Johan Peekstok		X	X						
Netwerk Netcentrisch Werken		X	X						
Ab van den Berg			X						
Regiegroep Netcentrisch Werken			X						

Accordering document

Namens Directie IFV

……
Wim Papperse
Directeur Bedrijfsvoering

Inhoud

1 Inleiding

Netcentrisch Werken richt zich op de informatievoorziening tijdens rampen en crises. De informatie die gebruikt wordt tijdens de bestrijding van (en voorbereiding op) rampen en crises moet beschikbaar, toegankelijk en bruikbaar zijn. Daarnaast moet deze informatie kunnen worden uitgewisseld tussen disciplines (hulporganisaties en crisispartners) en regio's. Om deze doelstellingen te ondersteunen wordt gebruik gemaakt van het Landelijk Crisis Management Systeem (LCMS).
In het referentiekader Netcentrische Crisisbeheersing wordt informatiebeveiliging beschouwd als een van de kritische succesfactoren voor Netcentrisch Werken.

1.1 Doel van dit document

Het doel van dit document is het beleidskader toegangsbeveiliging voor LCMS te documenteren. Dit beleidskader heeft als doel te waarborgen dat alleen bevoegde gebruikers toegang hebben tot de informatie die in LCMS is vastgelegd. Het beleidskader geeft aan ***wat*** er geregeld moet worden m.b.t. toegangsbeveiliging, niet ***hoe*** dit geregeld wordt.
Het beleidskader biedt:

> de richtlijn voor het opstellen van procedures met betrekking tot toegangsbeveiliging;
> richtlijnen voor gebruikers (zie 3.4 Eisen aan gebruikers) en beheerders.

Op basis van het beleidskader kunnen processen, procedures en ICT maatregelen worden gedefinieerd. Pas nadat deze zijn geïmplementeerd, kan aan de veiligheidsregio's en LOCC/NCC de zekerheid worden geboden dat alleen geautoriseerde gebruikers toegang krijgen tot het LCMS.

1.2 Scope

Het beleidskader toegangsbeveiliging LCMS is gebaseerd op de implementatierichtlijnen uit hoofdstuk 9 (toegangsbeveiliging) uit de NEN-ISO/IEC 27002 norm, met uitzondering van de paragrafen '9.1.2 Toegang tot netwerken en netwerkdiensten', '9.4.4 Speciale systeemhulpmiddelen gebruiken' en '9.4.5 Toegangsbeveiliging op programmabroncode'[1].

Het beleidskader omvat de volgende onderwerpen:

> welke personen toegang kunnen krijgen tot LCMS;
> waarvoor mogen gebruikers de informatie in LCMS gebruiken;
> welke eisen worden er gesteld aan de toegangsverleningsprocedure;
> waar worden gebruikers geacht zich aan te houden;
> welke eisen worden er aan wachtwoorden en inlogprocedures gesteld;
> welke eisen worden gesteld aan beheer van toegangsrechten en speciale (= beheer) rechten.

[1] Deze paragrafen hebben betrekking op toegang anders dan tot de applicatie (maar tot resp. het systeem waarop de applicatie draait, tooling voor het technisch beheer van de applicatie en de broncode van de applicatie).

1.3 Referenties

Het beleidskader toegangsbeveiliging LCMS is gebaseerd op de onderstaande richtlijnen en standaarden:

Titel	Versie	Auteur	Vindplaats
Referentiekader Netcentrische Crisisbeheersing	1.0.2 (27-09-201	Werkgroep Netcentrische Werkwijze	http://www.infopuntveiligheid.nl/Publicatie/DossierItem/7/4163/referentiekader-netcentrische-crisisbeheersing.html
NEN-ISO/IEC 27002	2013	Nederlands Normalisatie-instituut	http://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270022013-nl.htm
ICT-Beveiligingsrichtlijnen voor webapplicaties Deel 2	Januari 2012	Nationaal Cyber Security Centrum	https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers
Overbruggingsopdracht LCMS	24 april 2012	Johan Peekstok	
Besluit Veiligheidsregio's	24 oktober 2010		http://wetten.overheid.nl/BWBR0027844
Wet Veiligheidsregio's	11 februari 2010		http://wetten.overheid.nl/BWBR0027466
Concept Handreiking aansluiten crisispartners	0.5 (12-06-2014)	werkgroep Ketenpartners Netwerk Netcentrisch Werke	Virtueel kantoor
Guideline for Information Asset Valuation	07-09-2009	Mohan Kamat	The ISO 27K Forum (http://www.iso27001security.com)
Voorschrift informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIRBI)	2013		http://wetten.overheid.nl/BWBR0033507
Baseline Informatiebeveiliging Rijksdienst (BIR)	1.0 (1-12-2012)		http://www.earonline.nl/
Beveiliging van persoons-gegevens; Achtergrondstudies en Verkenningen 23	April 2001	G.W. van Blarkom drs. J.J. Borking	http://www.cbpweb.nl/downloads_av
Richtsnoeren 'Beveiliging van Persoonsgegevens'	19 februari 2013	College bescherming persoonsgegevens	www.cbpweb.nl

2 Uitgangspunten

2.1 Verantwoordelijkheden

Het IFV is eigenaar van het LCMS en daarmee primair verantwoordelijk voor het opstellen en implementeren van het beleidskader toegangsbeveiliging, het monitoren op de naleving hiervan en het nemen van maatregelen op basis van de gedane bevindingen.
De veiligheidsregio's en LOCC/NCC nemen de dienst voor het gebruik van LCMS af van het IFV. De afspraken hierover worden geregeld in de DNO (Diensten Niveau Overeenkomst) en de SLA (Service Level Agreement). Hierin wordt overeengekomen dat de veiligheidsregio's en LOCC/NCC gerechtigd zijn om toegang tot LCMS te verlenen aan gebruikers in hun eigen regio. Daarmee zijn zij impliciet mede verantwoordelijk voor het opstellen, controleren en handhaven van de procedures waarmee het beleidskader toegangsbeveiliging wordt uitgevoerd.

2.2 Wet en regelgeving

Het beleidskader toegangsbeveiliging LCMS houdt rekening met de Nederlandse wet- en regelgeving. Hierbij van toepassing zijn:
> Artikel 138ab van het wetboek van strafrecht;
> Artikel 272 van het wetboek van strafrecht;
> Wet bescherming persoonsgegevens;
> Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR);
> Beveiligingsvoorschrift Rijksdienst 2013;
> Voorschrift informatiebeveiliging Rijksdienst – Bijzondere Informatie 2013 (VIRBI);
> Baseline Informatiebeveiliging Rijksdienst 2012 (BIR);
> Richtsnoeren 'Beveiliging van Persoonsgegevens' 2013.

2.3 Informatie in LCMS

LCMS is een geautomatiseerd systeem dat het proces Operationeel Informatie Management via een netcentrische werkwijze ondersteunt. Dit proces ondersteunt het proces Leiding en Coördinatie via het maken en bijhouden van een actueel gedeeld beeld. Dit actuele gedeeld beeld is in het LCMS geïmplementeerd in 'activiteiten'.
Elke activiteit bestaat uit een tekstueel beeld en (optioneel) een grafisch beeld.
Een activiteit is opgebouwd uit:
> het situatiebeeld;
> het eigen beeld van de onderdelen van de hoofdstructuur van de rampenbestrijding en crisisbeheersing;
> de eigen beelden van de monodisciplinaire processen die de (voorbereiding op) de rampenbestrijding en crisisbeheersing ondersteunen (brandweerzorg, politiezorg, geneeskundige zorg, bevolkingszorg en crisiscommunicatie).

Het situatiebeeld is opgebouwd uit (geselecteerde onderdelen van) de eigen beelden. Dit geld voor zowel het tekstuele als het grafisch beeld.
Deze beelden worden via het LCMS gedeeld met:
> de onderdelen van de hoofdstructuur van de rampenbestrijding en crisisbeheersing
> andere bij de ramp of crisis betrokken partijen, voor zover zij deze gegevens nodig hebben voor de uitvoering van hun taken en bevoegdheden.
> de minister

(zie Besluit Veiligheidsregio's Artikel 2.4.1 en 2.4.2.)

2.4 Vertrouwelijkheid van de informatie

De informatie die in LCMS wordt gedeeld bevat in principe geen vertrouwelijke en privacy gevoelige informatie. Voor een goed verloop van de rampenbestrijding en crisisbeheersing, dient de informatie echter niet publiek toegankelijk te zijn, maar alleen beschikbaar voor professioneel gebruik.
7/22
Voor de security classificatie wordt gebruik gemaakt van de rubricering conform Mahat [Mahat 2009]. De security classificatie van de informatie in LCMS is als “Alleen intern gebruik” geclassificeerd (zie Bijlage B Security Classificatie).
In het Beleidskader Toegangsbeveiliging worden die implementatierichtlijnen uit de NEN-ISO/IEC 27002 norm overgenomen, die passen bij deze security classificatie.

3 Beleidseisen m.b.t. toegangsbeveiliging

In dit hoofdstuk staat het beleidskader toegangsbeveiliging van LCMS beschreven. In dit beleid zijn de eisen voor alle onderwerpen in het kader van toegangsbeveiliging vermeld conform de NEN-ISO/IEC 27002 standaard. Bij elke eis is de rationale opgenomen. Indien van toepassing is hier een verwijzing naar de toepasselijke norm opgenomen.

3.1 Toegestane gebruikers

Voor het beleidskader toegangsbeveiliging is het essentieel vast te stellen wie toegang tot het systeem mag krijgen [NEN-ISO/IEC 27002-9.1.1].

Nr.	Eis	Rationale
1.	De toegang tot LCMS wordt alleen verleend aan medewerkers die betrokken zijn bij (de voorbereiding op) de rampenbestrijding en crisisbeheersing. Hierbij wordt onderscheid gemaakt tussen: a) medewerkers die deel uitmaken van de hoofdstructuur van de crisisorganisatie en een rol hebben bij het opstellen van totaalbeeld en de eigen beelden. b) medewerkers van organisaties die betrokken zijn of kunnen worden bij de crisisbeheersing en rampenbestrijding (crisispartners). c) Medewerkers die betrokken zijn in de voorbereiding (planvorming) d) Medewerkers die betrokken zijn bij opleiden, trainen en oefenen (OTO). e) Medewerkers met speciale bevoegdheden m.b.t. de inrichting van het systeem. IFV, veiligheidsregio's en LOCC/NCC zijn gerechtigd om toegang te verlenen aan gebruikers van hun eigen organisatie en aan medewerkers van crisispartners die hieraan voldoen.	Op deze wijze kan invulling worden gegeven aan het besluit veiligheidsregio's.
2.	Alleen medewerkers van crisispartners die zijn aangesloten conform de 'handreiking aansluiten van crisispartners op de crisisorganisatie' kunnen toegang krijgen tot LCMS. De rechten die aan deze medewerkers worden toegekend, komen overeen met hetgeen in de handreiking is opgesteld.	[NEN-ISO/IEC 27002-9.2.2 / a] Veiligheidsregio's en LOCC/NCC zijn verantwoordelijk voor het aansluiten van crisispartners. Het IFV is echter eigenaar van het LCMS en daarmee primair verantwoordelijk voor het opstellen en implementeren van het beleidskader toegangsbeveiliging. Via de handreiking heeft het IFV een richtlijn om verleende toegang en toegangsrechten te monitoren en te controleren.
3.	Elke gebruiker van LCMS is herleidbaar tot een persoon waarvan kan worden geverifieerd dat deze terecht toegang heeft tot LCMS.	[NEN-ISO/IEC 27002-9.1.1 / f] Hierdoor kunnen gebruikers verantwoordelijk worden gesteld voor hun acties in het systeem.
4.	Personen die zich ongeautoriseerd toegang verschaffen tot LCMS zijn strafbaar volgens art. Artikel 138ab van het wetboek van strafrecht.	Het beleidskader toegangsbeveiliging is houdt rekening met Nederlandse wet- en regelgeving. [NEN-ISO/IEC 27002-9.1.1 / d]

3.2 Gebruik van gegevens

Voor het beleidskader toegangsbeveiliging is het essentieel beleidsregels voor informatieverspreiding en –autorisatie vast te stellen [NEN-ISO/IEC 27002-9.1.1 / b].

Nr.	Eis	Rationale
1.	De informatie in LCMS is alleen voor intern gebruik. Dit houdt in dat de informatie in LCMS alleen gebruikt worden mag ten behoeve van de crisisbeheersing en rampenbestrijding en de voorbereiding daarop. > Evaluaties, testen, pilots etc. worden in dit kader gezien als voorbereiding op de crisisbeheersing en rampenbestrijding. > Het beschikbaar stellen van informatie uit LCMS aan andere systemen is toegestaan als deze informatie gebruikt wordt ten behoeve van de crisisbeheersing en rampenbestrijding en de voorbereiding daarop.	[NEN-ISO/IEC 27002-9.1.1 / b] Voortijdig bekend raken van specifieke informatie kan leiden tot hindering van de rampenbestrijding en crisisbestrijding (bijv. ramptoerisme etc.).
2.	Medewerkers die toegang verkrijgen tot LCMS hebben een verklaring ondertekend waarin wordt gesteld dat ze vertrouwelijk omgaan met de informatie waartoe men toegang verkrijgt.	[NEN-ISO/IEC 27002-9.2.4 / a] Ongeautoriseerd gebruik of verspreiding van de informatie in het systeem wordt gezien als ‘ het schenden van een geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren’ (art. 272 wetboek van strafrecht). Voor ambtenaren en medewerkers van ZBO’s is dit gedekt door de arbeidsovereenkomst. Voor medewerkers van crisispartners dient dit te worden geregeld via de aansluitovereenkomst. Zonder vastlegging van de verklaring is er geen juridische basis voor sancties bij oneigenlijk gebruik van de gegevens.

3.3 Eisen aan toegangsverleningsprocedure

Het IFV is eindverantwoordelijk voor het toegangsbeveiligingsbeleid. Daarmee is het IFV tevens verantwoordelijk voor het opstellen van de eisen aan de toegangsverleningsprocedure.
De uitvoering van de toegangsverlening valt onder de verantwoordelijkheid van de IFV, Veiligheidsregio’s en LOCC / NCC. Ieder van deze organisaties hanteert een toegangsverleningsprocedure die voldoet aan de onderstaande eisen. Het IFV is verantwoordelijk voor de controle en monitoring op de naleving van deze eisen.

Nr.	Eis	Rationale
1.	De toegangsverleningsprocedure IFV, veiligheidsregio’s en LOCC / NCC is beschreven en goedgekeurd door de directie van het IFV.	[NEN-ISO/IEC 27002-9.1.1] Voor controle en monitoring is het noodzakelijk dat de gehanteerde procedures beschreven en vastgesteld zijn.
2.	De toegangsverleningsprocedure dient te waarborgen dat het indienen van een verzoek tot toegang, het beoordelen van het verzoek tot toegang en het verlenen van de daadwerkelijke toegang tot LCMS gescheiden taken zijn;	Door scheiding van taken wordt de kans op het verlenen van toegang aan ongewenste personen verminderd. [NEN-ISO/IEC 27002-9.1.1 / f]
3.	De toegangsverleningsprocedure dient te waarborgen dat aan de eisen m.b.t. toegestane gebruikers, gebruik van gegevens, eisen aan gebruikers en wachtwoorden wordt voldaan;	[NEN-ISO/IEC 27002-9.1.1 / g]
4.	De toegangsverleningsprocedure dient te waarborgen dat de toegang tot LCMS alleen wordt verleend door	[NEN-ISO/IEC 27002-9.1.1 / g] Op deze manier is de toegangsverleningsprocedure een stuurbaar proces.

Nr.	Eis	Rationale
	speciaal daartoe aangewezen medewerkers (landelijk of regionale beheerders);	
5.	De toegangsverleningsprocedure dient te waarborgen dat er vastgestelde en door IFV goedgekeurde criteria zijn waaraan de toegangsverlening wordt getoetst. Deze criteria geven aan: > of een medewerker recht heeft op toegang tot LCMS; > tot welke informatie de medewerker toegang mag krijgen; > of de medewerker alleen kan lezen of ook gegevens mag wijzigen.	[NEN-ISO/IEC 27002-9.1.1 / g] [NEN-ISO/IEC 27002-9.2.2 / a] Het IFV is als eigenaar van LCMS eindverantwoordelijk voor het handhaven van het beleidskader toegangsbeveiliging. Voor het controleren en monitoren is het nodig dat de criteria goed omschreven zijn.
6.	De toegangsverleningsprocedure dient te waarborgen dat er een registratie wordt bijgehouden waarin is vastgelegd aan welke personen van welke organisatie toegang is verleend en welke autorisatie, wie de aanvraag daarvoor heeft gedaan, wie de goedkeuring heeft verleend en op basis van welke criteria en wie de toegang heeft verleend. Deze registratie is beschikbaar voor het IFV en direct opvraagbaar.	Op deze manier kan achteraf worden gecontroleerd of de toekenning volgens de procedure is verlopen. [NEN-ISO/IEC 27002-9.1.1 / j] [NEN-ISO/IEC 27002-9.2.2 / d j]
7.	De toegangsverleningsprocedure dient te waarborgen dat gebruikers een persoonlijke gebruikersidentificatie ontvangen die uniek is binnen de organisatie die de toegang verleent.	Hierdoor kunnen gebruikers worden gekoppeld aan en verantwoordelijk worden gesteld voor hun acties in het systeem. [NEN-ISO/IEC 27002-9.2.1 / a]
8.	De toegangsverleningsprocedure dient te waarborgen dat gebruikers geen gebruikersidentificatie ontvangen die eerder aan een andere gebruiker is toegekend.	[NEN-ISO/IEC 27002-9.2.1 / d] Het koppelen van acties in het systeem aan personen wordt hierdoor anders nodeloos ingewikkeld.
9.	De toegangsverleningsprocedure dient te waarborgen dat gebruikers een initieel wachtwoord ontvangen t.b.v. de authenticatie. Dit initiële wachtwoord voldoet aan de eisen aan wachtwoorden en dient verplicht te worden gewijzigd bij de eerste keer inloggen.	[NEN-ISO/IEC 27002-9.2.4 / b, e] Het wachtwoord is strikt persoonlijk en dient ook niet bij de beheerder bekend te zijn.
10.	De toegangsverleningsprocedure dient te waarborgen dat wachtwoorden op een veilige manier aan gebruikers worden gegeven (dus bijv. niet ongecodeerd via mail verstuurd). Veilige(re) manieren zijn bijv. gecodeerde e-mail, persoonlijk overhandigen, telefonisch.	[NEN-ISO/IEC 27002-9.2.4 / d] [NEN-ISO/IEC 27002-9.4.3 / i] Hierdoor wordt voorkomen dat misbruik kan worden gemaakt van het onderscheppen van de wachtwoorden.
11.	De toegangsverleningsprocedure dient te waarborgen dat de identiteit van een gebruiker eerst wordt vastgesteld, voordat een (nieuw) initieel wachtwoord wordt verstrekt.	Op deze manier wordt de kans verkleind dat wachtwoorden worden verstrekt aan personen die zich voordoen als iemand anders. [NEN-ISO/IEC 27002-9.2.4 / c]
12.	De toegangsverleningsprocedure dient te waarborgen dat de ontvangst van een wachtwoord door de gebruiker te wordt bevestigd.	Hierdoor wordt gewaarborgd dat het wachtwoord bij de juiste gebruiker terecht komt. [NEN-ISO/IEC 27002-9.2.4 / f]

3.4 Eisen aan gebruikers

Gebruikers die toegang krijgen tot LCMS zijn verantwoordelijk voor het beschermen van hun authenticatie informatie. Van gebruikers wordt verwacht dat zij zich houden aan de onderstaande voorwaarden voor gebruik van LCMS. Elke gebruiker dient derhalve te beschikken over deze voorwaarden, c.q. moet eenvoudig deze voorwaarden kunnen opvragen. De naleving van deze voorwaarden is primair de verantwoordelijkheid van de gebruiker.

Nr.	Eis	Rationale
1.	Gebruikers van LCMS behoren vertrouwelijk om te gaan met de informatie die zij via LCMS tot hun beschikking krijgen en dienen hiervoor een verklaring te ondertekenen.	[NEN-ISO/IEC 27002-9.2.4 / a] Deze verklaring kan zijn opgenomen in de arbeidsvoorwaarden en de convenanten tussen IFV, veiligheidsregio's en crisispartners.
2.	Gebruikers dienen vertrouwelijk om te gaan met de authenticatie informatie die ze hebben gekregen om toegang te verkrijgen tot LCMS en er voor te zorgen dat deze niet openbaar anderszins bekend wordt bij derden.	Hierdoor wordt de kans verkleind dat ongeautoriseerde personen zich met het account van een geautoriseerde gebruiker toegang verschaffen tot LCMS. [NEN-ISO/IEC 27002-9.3.1 / a]
3.	Gebruikers van LCMS behoren het wachtwoord niet te registreren (papier, mobiel device, computerbestand) tenzij op een wijze die niet voor anderen toegankelijk is en die door de eigen organisatie is goedgekeurd.	Hierdoor wordt de kans verkleind dat derden zich toegang verschaffen middels een bestaand account. [NEN-ISO/IEC 27002-9.3.1 / b]
4.	Gebruikers van LCMS behoren het wachtwoord te wijzigen zodra er een aanwijzing is dat dit bekend is of kan worden bij derden.	Hierdoor wordt de kans verkleind dat derden zich toegang verschaffen middels een bestaand account. [NEN-ISO/IEC 27002-9.3.1 / c]
5.	Gebruikers van LCMS behoren een wachtwoord te kiezen dat sterk is, gemakkelijk te onthouden is en niet gemakkelijk door een derde geraden kan worden. > Makkelijk te raden wachtwoorden zijn bijvoorbeeld: – gebaseerd op persoons gerelateerde gegevens die makkelijk door anderen te achterhalen zijn (zoals namen van familie, vrienden, collega's, huisdieren, geboortedatums, telefoonnummers etc.); – een vast woord, gevolgd door een volgnummer dat bij iedere wachtwoordwijziging wordt opgehoogd; – uit opeenvolgende identieke tekens bestaat (zoals aaaaaa 1234 qwerty etc.); – een woord uit een woordenboek. > Wachtwoorden kunnen gemakkelijker worden onthouden als ze gebaseerd zijn op een zin. Bijvoorbeeld de zin 'Denkend aan Holland zie ik brede rivieren traag door oneindig laagland gaan' wordt dan 'd@Hz1brtd0lg'; > Sterke wachtwoorden zijn wachtwoorden die voldoen aan de eisen in paragraaf 3.5 Eisen aan beheer van wachtwoorden.	[NEN-ISO/IEC 27002-9.3.1 / d]Sterke en moeilijk te raden wachtwoorden zijn minder snel door 'trial & error' te achterhalen. Door een wachtwoord te kiezen dat voor de gebruiker makkelijk te onthouden is, is er minder kans dat men het wachtwoord noteert (met het risico dat dit door een derde wordt achterhaald).
6.	Gebruikers van LCMS behoren alleen gebruik te maken van de aan hen toegekende gebruikersidentificatie om toegang te krijgen tot LCMS. Het gebruik van de gebruikersidentificatie van een ander is niet toegestaan.	Alleen op deze wijze is achteraf te bepalen wie welke handelingen in het systeem heeft verricht. [NEN-ISO/IEC 27002-9.4.3 / e]
7.	Gebruikers dienen voor aanvullende maatregelen te zorgen voor de bescherming van wachtwoorden wanneer deze worden gebruikt voor geautomatiseerde inlogprocedures. De gekozen bescherming moet goedgekeurd worden door het IFV.	[NEN-ISO/IEC 27002-9.4.3 / f] In specifieke situatie kan het zijn dat wordt ingelogd via een geautomatiseerd inlogscript (bijv. Plot Mobiel). Deze inlogmethode dient voldoende beschermd te zijn om te voorkomen dat deze door derden gebruikt kan worden.
8.	Gebruikers van LCMS behoren geen wachtwoord te kiezen dat ook voor particuliere toepassingen wordt gebruikt.	Hierdoor wordt voorkomen dat wachtwoorden bekend raken als particuliere toepassingen worden 'gekraakt'. [NEN-ISO/IEC 27002-9.3.1 / g]
9.	Gebruikers van LCMS dienen alert te zijn op misbruik van de aan hen toegekende gebruikersidentificatie en bij vermoeden van misbruik hiervan melding te maken.	De gebruiker maakt zelf ook deel uit van de beveiligde inlogprocedure en heeft hierin een verantwoordelijkheid m.b.t. monitoring en signalering. [NEN-ISO/IEC 27002-9.4.2 / g]

3.5 Eisen aan beheer van wachtwoorden

Voor het beleidskader toegangsbeveiliging is het essentieel beleidsregels voor het beheer van wachtwoorden te stellen [NEN-ISO/IEC 27002-9.4.3].

Nr.	Eis	Rationale
1.	Een wachtwoord in LCMS dient te voldoen aan de volgende eisen: > een wachtwoord bestaat uit minimaal 8 karakters; > een wachtwoord bevat minstens 3 van de volgende soorten tekens: – kleine letters – hoofdletters – cijfers – speciale tekens !@#$%&*()_-+={[}]|\;:,<.>/?; > een wachtwoord mag niet door meer dan 5 andere gebruikers gebruikt worden.	[NEN-ISO/IEC 27002-9.3.1 / d] [NEN-ISO/IEC 27002-9.4.3 / c] Sterke en moeilijk te raden wachtwoorden zijn minder snel door 'trial & error' te achterhalen. Deze eis stelt gangbare minimum criteria voor sterke wachtwoorden. Als meerdere gebruikers eenzelfde wachtwoord kiezen is dit een aanwijzing dat het wachtwoord ook gemakkelijk te raden is.
2.	Het initiële wachtwoord dient direct bij de eerste keer inloggen aangepast te worden.	Het initiële wachtwoord is ook bekend bij de persoon die het wachtwoord uitgeeft. Door het direct aan te passen wordt het wachtwoord weer strikt persoonlijk. [NEN-ISO/IEC 27002-9.4.3 / d]
3.	Gebruikers mogen hun wachtwoord onbeperkt wijzigen.	Beperkingen aan de frequentie waarmee wachtwoorden mogen worden gewijzigd kan een drempel opwerpen voor gebruikers om hun wachtwoord regelmatig te wijzigen. [NEN-ISO/IEC 27002-9.4.3 / b]
4.	Een wachtwoord dient minimaal elke 6 maanden te worden gewijzigd.	[NEN-ISO/IEC 27002-9.4.3 / e] Door een minimum frequentie in te stellen waarmee wachtwoorden gewijzigd worden, wordt de kans op gecompromitteerde wachtwoorden verkleind en worden gebruikers alert gehouden op de toegangsbeveiliging. Uitgangspunt is dat gebruikers minimaal 2 maal per jaar in te loggen in het systeem t.b.v. OTO. Gebruikers die weinig inloggen zijn eerder geneigd om wachtwoorden op te schrijven. Door deze maatregel wordt de kans verkleind dat een wachtwoord is gecompromitteerd.
5.	Een wachtwoord mag niet binnen twee jaar of 5 wijzigingen nogmaals worden gebruikt door dezelfde gebruiker.	Op deze manier wordt de kans verkleind dat een gecompromitteerd wachtwoord alsnog misbruikt kan worden. [NEN-ISO/IEC 27002-9.4.3 / f]

3.6 Eisen aan inloggen

Om onbevoegde toegang tot LCMS te voorkomen, dienen gebruikers zich te identificeren en te authentiseren via een inlogprocedure [NEN-ISO/IEC 27002-9.4.2]. Aan deze inlogprocedure worden de volgende eisen gesteld:

Nr.	Eis	Rationale
1.	Gebruikers identificeren zich tijdens het inloggen met de persoonlijke gebruikersidentificatie die ze hebben ontvangen.	Hierdoor kunnen gebruikers worden gekoppeld aan en verantwoordelijk worden gesteld voor hun acties in het systeem. [NEN-ISO/IEC 27002-9.2.1/ a]
2.	Tijdens de inlogprocedure worden geen identificatoren van het systeem (bijv. de URL) getoond voordat het inlogproces succesvol is afgerond.	De kans op geautomatiseerde aanvallen op het systeem is kleiner als de identificatoren niet openbaar zijn. [NEN-ISO/IEC 27002-9.4.2 / a]

Nr.	Eis	Rationale
3.	Tijdens de inlogprocedure wordt een algemene waarschuwing getoond dat: > de applicatie alleen toegankelijk is voor geautoriseerde gebruikers; > het ongeautoriseerd toegang verschaffen strafbaar is; > geautoriseerde gebruikers zelf verantwoordelijk zijn voor het geheim houden van hun inloggegevens.	Hierdoor wordt de awareness van de gebruiker op de vertrouwelijkheid van de gegevens bij elke inlogmoment geprikkeld. (N.B. de meeste gebruikers van LCMS zullen slechts een beperkt aantal keer per jaar inloggen). [NEN-ISO/IEC 27002-9.4.2 / b]
4.	Gebruikers die de eerste keer inloggen nadat ze een nieuw wachtwoord hebben ontvangen dienen na het succesvol inloggen hun wachtwoord te wijzigen.	Hierdoor kunnen gebruikers een door hun makkelijker te onthouden wachtwoord kiezen, waardoor de kans dat ze het wachtwoord vergeten verminderd wordt. Daarnaast wordt de kans op misbruik van een verstrekt initieel wachtwoord verkleind, doordat dit maar een beperkte periode actief is. [NEN-ISO/IEC 27002-9.2.4 / b] Zie ook punt 2 in par 3.5 en Punt 9 in par 3.3
5.	Tijdens de inlogprocedures worden geen hulpboodschappen getoond waarmee onbevoegde gebruikers geholpen kunnen worden	Onbevoegde toegang tot LCMS wordt hierdoor niet makkelijker gemaakt. Geautoriseerde gebruikers worden geacht de inlogprocedure te kennen. [NEN-ISO/IEC 27002-9.4.2 / c]
6.	Validatie van de ingevoerde inloggegevens vindt pas plaats nadat alle gegevens zijn ingevoerd. Indien deze niet juist zijn, geeft het systeem niet aan welk deel van de invoer onjuist is.	Uit de stapsgewijze validatie is af te leiden welke van de ingevoerde gegevens onjuist zijn (bijv. of het wel of niet een bestaande identificatie betreft). [NEN-ISO/IEC 27002-9.4.2 / d]
7.	Na vijfmaal achtereen foutief inloggen wordt de gebruiker geblokkeerd. Deze blokkering is alleen door een beheerder op te heffen, waarbij er een nieuw initieel wachtwoord wordt verstrekt.	De inlogprocedure is robuust tegen inlogpogingen met ‘grove middelen’ (bijv. geautomatiseerde inlogpogingen). [NEN-ISO/IEC 27002-9.4.2 / e]
8.	Zowel succesvolle als niet-succesvolle inlogpogingen worden geregistreerd.	[NEN-ISO/IEC 27002-9.4.2 / f]
9.	Gebruikers authentiseren zich bij het inloggen middels een geheim wachtwoord.	Tweeweg authenticatie (kennis + bezit) is een krachtiger middel dan éénweg authenticatie (alleen kennis, bijv. een wachtwoord). De kracht van de authenticatie dient in overeenstemming te zijn met de classificatie van de te beveiligen informatie. Aangezien de security classificatie van de informatie in LCMS als ‘alleen intern gebruik’ wordt geclassificeerd, wordt éénweg authenticatie als afdoende beveiliging beschouwd. [NEN-ISO/IEC 27002-9.4.2]
10.	Gebruikers die hun wachtwoord niet meer weten, kunnen een nieuwe initieel wachtwoord aanvragen. Dit wachtwoord kan ook op geautomatiseerde wijze worden gegenereerd (i.e. zonder tussenkomst van een beheerder).	In crisissituaties is het van belang dat gebruikers snel toegang hebben tot het systeem. Via geautomatiseerde wachtwoord reset kunnen gebruikers sneller hun toegang herstellen dan via een procedure met menselijke tussenkomst (via beheerders). [NEN-ISO/IEC 27002-9.4.3 / b]
11.	Inlogpogingen worden gemonitord waarbij signalering van pogingen tot doorbreken van de beveiligingsprocedures plaatsvindt. Bij herhaalde signaleringen wordt gerapporteerd aan het IFV, dat hierop maatregelen initieert.	Zonder monitoring en signalering zijn beveiligde inlogprocedures uiteindelijk te doorbreken. Zonder responsprocedures heeft monitoring en signalering geen zin. [NEN-ISO/IEC 27002-9.4.2 / g]
12.	Nadat een gebruiker succesvol is ingelogd krijgt deze de volgende gegevens te zien: > datum/tijd van de vorige succesvolle inlogpoging; > datum/tijd van alle niet-succesvolle inlogpogingen sinds de vorige succesvolle inlogpoging.	Gebruikers zijn op deze wijze in staat om te controleren dat niet door een derde gebruik is gemaakt van hun account, [NEN-ISO/IEC 27002-9.4.2 / h]
13.	Tijdens het invoeren van het wachtwoord wordt dit niet op het scherm getoond.	Het risico dat derden het wachtwoord achterhalen door ‘over de schouder mee te kijken’ wordt hierdoor verminderd. [NEN-ISO/IEC 27002-9.4.2 / i]

Nr.	Eis	Rationale
14.	Ingevoerde wachtwoorden worden niet ongecodeerd over het netwerk verstuurd.	Het moet niet mogelijk zijn om via onderschepping van het netwerkverkeer de ingevoerde wachtwoorden te onderscheppen. [NEN-ISO/IEC 27002-9.4.2 / j]
15.	De sessie met het systeem wordt beëindigd als gebruikers gedurende een bepaalde (instelbare) tijd niet actief zijn in het systeem.	Als sessies niet automatisch worden beëindigd, bestaat de kans dat bij aflossing van medewerkers de nieuwe medewerker verder gaat met de sessie van zijn voorganger. In dat geval zijn de acties in het systeem niet meer herleidbaar tot een (juiste) persoon. Met deze maatregel wordt de kans hierop verkleind. [NEN-ISO/IEC 27002-9.4.2 / k]

3.7 Beheer van toegangsrechten

De toegangsrechten van alle medewerkers en externe gebruikers van LCMS behoren te worden beheerd. Hieronder wordt verstaan: aanpassing van de rechten bij wijzigingen van functie en beëindiging van de toegang bij beëindiging van dienstverband, contract of overeenkomst. [NEN-ISO/IEC 27002-9.2.6]

Nr.	Eis	Rationale
1.	IFV en veiligheidsregio´s beoordelen minimaal 1 maal per jaar of de criteria op basis waarvan de toegang en autorisatie is verleend aan gebruikers die binnen hun verantwoordelijkheid vallen, nog steeds van toepassing zijn en de toegang intrekken of de autorisatie aan te passen waar dat niet van toepassing is.	Op deze manier kan worden geborgd dat ook de toegang van gebruikers waarvan niet gemeld wordt dat ze uit dienst zijn of een andere functie hebben, word aangepast. [NEN-ISO/IEC 27002-9.1.1 / h] [NEN-ISO/IEC 27002-9.2.1 / c] [NEN-ISO/IEC 27002-9.2.5 / a]
2.	In de toegangsverleningsprocedure is opgenomen hoe gewaarborgd wordt dat de toegangsrechten van medewerkers van de eigen organisatie en van crisispartners, die uit dienst gaan of van functie veranderen, opnieuw worden beoordeeld en toegekend	Gebruikers die uit dienst gaan, zijn niet meer vatbaar voor sancties vanuit de eigen organisatie. Door het intrekken van de autorisaties wordt verhinderd dat er misbruik wordt gemaakt van de autorisatiegegevens van deze gebruikers. [NEN-ISO/IEC 27002-9.1.1 / h] [NEN-ISO/IEC 27002-9.2.1 / b] [NEN-ISO/IEC 27002-9.2.5 / b]
3.	De beheerprocedures voor het beheer van toegangsrechten dienen beschreven te zijn en goedgekeurd door het IFV.	[NEN-ISO/IEC 27002-9.2.2 / a]
4.	Bij een wijziging in de toegangsrechten van een gebruiker wordt geregistreerd wie die rechten heeft aangepast.	[NEN-ISO/IEC 27002-9.2.6]

3.8 Speciale toegangsrechten

Speciale toegangsrechten zijn toegangsrechten met autorisaties die los staan van operationeel gebruik van de informatie. Hieronder worden rechten verstaan waarmee systeem- of toepassingscontroles kunnen worden omzeild, aangepast of opgeheven. Dit betreft zowel toegangsrechten voor technisch beheer als functioneel beheer.
Het toewijzen en gebruik van deze speciale toegangsrechten dient te worden beperkt en beheerst [NEN-ISO/IEC 27002-9.2.3]. Ongepast gebruik van speciale rechten voor systeembeheer is een factor die in grote mate kan bijdragen aan storingen van of inbreuken op het systeem.

Voor het beheren van deze speciale toegangsrechten gelden onderstaande eisen:

Nr.	Eis	Rationale
1.	Alle speciale rechten (zowel t.b.v. technisch als functioneel beheer) en aan welk soort gebruikers ze dienen te worden toegekend, zijn geïdentificeerd, beschreven en ter beschikking van het IFV.	[NEN-ISO/IEC 27002-9.2.3 /a]
2.	Toekenning van de speciale rechten aan medewerkers vindt alleen plaats met expliciete goedkeuring door het IFV. Het IFV beoordeelt hierbij of de speciale rechten noodzakelijk zijn voor de uitoefening van hun functie.	[NEN-ISO/IEC 27002-9.2.3 /b]
3.	De toegangsverleningsprocedure voor speciale toegangsrechten voldoet verder aan alle eisen voor de procedure voor verlening van reguliere toegangsrechten.	[NEN-ISO/IEC 27002-9.2.3 /c]
4.	Speciale toegangsrechten binnen LCMS mogen worden toegekend aan gebruikersidentificaties die ook voor reguliere activiteiten worden gebruikt.	(Regionaal) beheerders binnen LCMS hebben vaak ook een operationele rol. In voorkomende situaties dienen deze medewerkers beide rollen gelijktijdig te kunnen vervullen. [NEN-ISO/IEC 27002-9.2.3 /e].
5.	Jaarlijks wordt geëvalueerd of de medewerkers met speciale toegangsrechten deze rechten nog nodig hebben voor hun taken, en of ze zijn toegerust voor het uitvoeren van die taken.	Technologische ontwikkelingen leiden er toe dat wijzigingen in middleware, operating systems, databases etc. plaats vinden. De kennis hierover dient op peil gehouden te worden om te voorkomen dat ondeskundig gebruik van de speciale toegangsrechten tot problemen verstoringen leidt. [NEN-ISO/IEC 27002-9.2.3 /f]
6.	Voor technisch beheer mogen geen algemene gebruikersidentificaties voor beheer (i.e. niet persoonlijke accounts) worden gebruikt, maar moet de beheerfaciliteit RBAC (Role Based Access Control) ondersteunen.	Hierdoor is niet nodig dat gebruikersidentificaties voor technisch beheer worden gedeeld en zijn wijzingen altijd naar personen te herleiden. [NEN-ISO/IEC 27002-9.2.3 /g]. Speciale maatregelen voor de geheimhouding van de authenticatie informatie van deze accounts zijn dan verder overbodig [NEN-ISO/IEC 27002-9.2.3 /h]

4 Begrippen

Aangesloten organisatie	Organisatie, anders dan IFV, Veiligheidsregio, LOCC en NCC, die een overeenkomst heeft met IFV of Veiligheidsregio over het gebruik van LCMS door medewerkers van die organisatie.
IFV	Het Instituut Fysieke Veiligheid zoals bedoeld in de Wet Veiligheidsregio's, art. 66-75.
RBAC	Role Based Access Control. Mechanisme waarbij de rechten van een gebruiker worden toegekend via de rol van de gebruiker.
Bijzondere informatie	Terminologie die in het 'Besluit Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie' (VIRBI) wordt gebruikt voor informatie waar kennisname door niet geautoriseerde nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries.
Bijzondere persoonsgegevens	Terminologie uit de 'Wet Bescherming Persoonsgegevens' (WBP) voor persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

5 Bijlage A: Traceability beleidsregels

In onderstaande tabel is aangegeven in welke beleidsregels van het beleidskader toegangsbeveiliging LCMS de richtlijnen voor beheersmaatregelen uit de NEN-ISO/IEC 27002 standaard zijn overgenomen.

Beleidsregel		ISO27002 par. 9.1.1	ISO27002 par. 9.1.2	ISO27002 par. 9.2.1	ISO27002 par. 9.2.2	ISO27002 par. 9.2.3	ISO27002 par. 9.2.4	ISO27002 par. 9.2.5	ISO27002 par. 9.2.6	ISO27002 par. 9.3.1	ISO27002 par. 9.4.1	ISO27002 par. 9.4.2	ISO27002 par. 9.4.3	ISO27002 par. 9.4.4	ISO27002 par. 9.4.5
Toegestane gebruikers	1	X													
	2	X			X										
	3	X													
	4	X													
Gebruik van gegevens	1	X													
	2						X								
Toegangsverleningsprocedure	1	X													
	2	X													
	3	X													
	4	X													
	5	X			X										
	6	X			X										
	7			X											
	8			X											
	9						X								
	10						X						X		
	11						X								
	12						X								
Gebruikers	1						X								
	2									X					
	3									X					
	4									X					
	5									X					
	6												X		
	7												X		
	8									X					
	9											X			
Wachtwoorden	1									X			X		
	2												X		
	3												X		
	4												X		
	5												X		

Beleidsregel		ISO27002 par. 9.1.1	ISO27002 par. 9.1.2	ISO27002 par. 9.2.1	ISO27002 par. 9.2.2	ISO27002 par. 9.2.3	ISO27002 par. 9.2.4	ISO27002 par. 9.2.5	ISO27002 par. 9.2.6	ISO27002 par. 9.3.1	ISO27002 par. 9.4.1	ISO27002 par. 9.4.2	ISO27002 par. 9.4.3	ISO27002 par. 9.4.4	ISO27002 par. 9.4.5
Inloggen	1			X											
	2											X			
	3											X			
	4											X			
	5											X			
	6											X			
	7											X			
	8											X			
	9											X			
	10												X		
	11											X			
	12											X			
	13											X			
	14											X			
	15											X			
Beheer van toegangsrechten	1	X		X				X	X						
	2	X		X				X	X						
	3				X				X						
	4								X						
Speciale toegangsrechten	1					X									
	2					X									
	3					X									
	4					X									
	5					X									
	6					X									

6 Bijlage B: Security Classificatie LCMS Informatie

Aan de informatie in LCMS wordt de security classificatie ‘alleen intern gebruik’ toegekend. Onderstaand wordt (in omgekeerde volgorde) toegelicht wat deze classficatie inhoud, welke classificatie methodiek hieraan ten grondslag ligt en waarom niet voor een andere standaard classificaties gekozen is.

6.1 Gangbare classificaties

Voor de classificatie (of rubricering) van de vertrouwelijkheid van informatie bestaan diverse richtlijnen vanuit de overheid:

> Het Besluit Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIRBI) geeft een rubricering van als ‘bijzondere informatie’. Deze bijzondere informatie wordt gedefinieerd als:
  – Informatie waar kennisname door niet geautoriseerden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries;
> In de Wet Bescherming Persoonsgegevens, wordt binnen de ‘persoonsgegevens’ de categorie ‘bijzondere persoonsgegevens’ onderscheiden:
  – Gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag;
> In de Baseline Informatiebeveiliging Rijksdienst (BIR) is het basisvertrouwelijkheids-niveau voor informatie binnen de rijksoverheid (departementen) vastgesteld op “Departementaal Vertrouwelijk” (conform de rubricering van ‘bijzondere informatie’ in de VIRBI) en vertrouwelijkheidniveau WBP-risicoklasse 2 (conform ‘Beveiliging van persoonsgegevens; Achtergrondstudies en Verkenningen 23’). Deze risicoklasse wordt echter sinds het uitkomen van de ‘Richtsnoeren Beveiliging van Persoonsgegevens’ niet meer gehanteerd;
> Het ISO27K Forum stelt een toolkit beschikbaar met diverse best practices, waaronder voor security classificatie (Kamat 2009).

6.2 Keuze voor classificatie

De informatie die in LCMS wordt gedeeld bevat in principe ***geen*** vertrouwelijke en privacy gevoelige informatie. De informatie in LCMS wordt derhalve ***niet*** gezien als ‘bijzondere informatie’ conform de definitie in de VIRBI of ‘bijzondere persoonsgegevens’ in de WBP. Het vertrouwelijkheidsniveau van de informatie in LCMS is daarmee ***lager*** dan het basisvertrouwelijkheidsniveau voor informatie binnen de rijksoverheid conform de BIR.

Zowel de WBP, de NEN/ISO 27002 norm als de ‘Richtsnoeren Beveiliging van Persoonsgegevens’ geven aan dat voor de security classificatie van informatie een risicogerichte benadering vereist is, waarbij op basis van de in kaart gebrachte risico’s de betrouwbaarheidseisen worden opgesteld. Dit traject is voor LCMS echter nooit uitgevoerd.

Voor het classificeren van de vertrouwelijkheid van de informatie in LCMS is daarom gebruik gemaakt van de indeling volgens [Kamat 2009]. Deze classificatie is een van de vele best practices die voor ISO27000 trajecten gebruikt worden. Het voordeel van deze classificatiemethodiek is dat ze eenvoudig en intuïtief is.

6.3 Uitleg Classificatie

Security Classificatie	Omschrijving
Vertrouwelijk	Indien deze informatie buiten de organisatie beschikbaar komt, leidt dit tot ernstige financiële of imago schade, of overtredingen van de wet. Toegang tot deze informatie wordt beperkt tot 'need-to-know' en vereist de toestemming van de informatie eigenaar.
Algemeen intern gebruik	Indien deze informatie buiten de organisatie beschikbaar komt, leidt dit tot verwaarloosbare financiële of imago schade en geen ernstige schade aan de organisatie. Toegang tot de informatie is vrij toegankelijk voor alle interne gebruikers.
Openbaar	Onbeschikbaarheid of openbaarmaking van de informatie heeft geen gevolgen voor de organisatie. Informatie kan publiek verspreid worden na goedkeuring van communicatie of marketing afdelingen.

Op basis bovenstaande is de security classificatie 'alleen intern gebruik' toegekend.