Veiligheidsregio
HOLLANDS MIDDEN
Samen sterk voor meer veiligheid!

netcentrischwerken
by crisisplein.nl

GEBRUIKERSVOORWAARDEN LCMS

Met het gebruik van het LCMS account stemt u in met deze Gebruikersvoorwaarden en geeft u aan dat u de inhoud van de voorwaarden kent en deze naleeft.

A) TOEGESTANE GEBRUIKERS

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
2. Alleen medewerkers van crisispartners die zijn aangesloten 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.
3. Elke gebruiker van LCMS is herleidbaar tot een persoon waarvan kan worden geverifieerd dat deze terecht toegang heeft tot LCMS.
4. Personen die zich ongeautoriseerd toegang verschaffen tot LCMS zijn strafbaar volgens art. Artikel 138ab van het wetboek van strafrecht.

B) GEBRUIK VAN GEGEVENS

De informatie in LCMS is alleen voor intern gebruik. Dit houdt in dat de informatie in LCMS alleen gebruikt mag worden 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.

C) TOEGANGVERLENINGSPROCEDURE

De procedure voor het verkrijgen, wijzigen1 of verwijderen van een LCMS account is als volgt:
   a) De eindgebruiker: de gebruiker van het account (zoals beschreven onder A - Toegestane gebruikers) dient een verzoek in bij zijn/haar Super User (eventueel via een piket coördinator).
   b) De Super User: een aangewezen kerngebruiker die de aanvraag beoordeelt, accordeert en indient bij de regionaal functioneel beheerder. Er zijn 7 Key Users, deze zijn gekoppeld aan de volgende gebruiksgroepen:
      - Brandweer
      - Gemeenten
      - GHOR
      - Politie
      - Meldkamer
      - Multidisciplinaire teams
      - Ketenpartners
   c) De Regionaal Functioneel Beheerder: de beheerder met systeemrechten die de accountverzoeken van de Key Users uitvoert. Het functioneel beheer van LCMS is belegd bij de afdeling IM van Brandweer Hollands Midden: functioneelbeheer@brandweer.vrhm.nl of 088 246 5555 (alleen tijdens kantoortijden)

---

1 Het herstellen van een wachtwoord valt niet onder het proces wijzigen; het gaat hier immers om het herstellen van een al geaccordeerd account. Dit verzoek kan daarom rechtsreeks naar de Regionaal Functioneel Beheerder.

GEMEENTEN Hollands Midden · GHOR · BRANDWEER Hollands Midden

D) EISEN AAN GEBRUIKERS

1. Gebruikers van LCMS behoren vertrouwelijk om te gaan met de informatie die zij via LCMS tot hun beschikking krijgen
2. Gebruikers dienen vertrouwelijk om te gaan met de accountinformatie die ze hebben gekregen om toegang te verkrijgen tot LCMS en er voor te zorgen dat deze niet openbaar anderszins bekend wordt bij derden.
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 (bijvoorbeeld Keepass).
4. Gebruikers van LCMS behoren het wachtwoord te wijzigen zodra er een aanwijzing is dat dit bekend is of kan worden bij derden.
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:
    a. gebaseerd op persoonsgerelateerde gegevens die makkelijk door anderen te achterhalen zijn (zoals namen van familie, vrienden, collega's, huisdieren, geboortedatums, telefoonnummers etc.)
    b. Een vast woord, aangevuld met een volgnummer dat bij iedere wachtwoordwijziging wordt opgehoogd.
    c. Uit opeenvolgende identieke tekens bestaat (zoals aaaaaa 1234 qwerty etc.)
    d. een woord uit een woordenboek

    Sterke wachtwoorden zijn wachtwoorden die voldoen aan de volgende eisen:
    a. een wachtwoord bestaat uit minimaal 8 karakters;
    b. een wachtwoord bevat minstens 3 van de volgende soorten tekens:
        - kleine letters
        - hoofdletters
        - cijfers
        - speciale tekens !@#$%&*()_-+={[}]|\;:,<.>/?;

    Een wachtwoord mag daarnaast niet door meer dan 5 andere gebruikers gebruikt worden. Dit is een indicatie dat het wachtwoord niet voldoet; in dit geval waarschuwt het systeem de beheerder.
6. Gebruikers van LCMS behoren alleen gebruik te maken van de aan hen persoonlijk toegekende gebruikersidentificatie om toegang te krijgen tot LCMS. Het gebruik van de gebruikersidentificatie van een ander is niet toegestaan.
7. Gebruikers van LCMS behoren geen wachtwoord te kiezen dat ook voor particuliere toepassingen wordt gebruikt.
8. Gebruikers van LCMS dienen alert te zijn op misbruik van de aan hen toegekende gebruikersidentificatie en bij vermoeden van misbruik hiervan melding te maken.
9. Gebruikers van LCMS dienen minimaal 1 x per 6 maanden met het account in te loggen. Wanneer dit niet wordt gedaan zal de regionaal functioneel beheerder het account ter controle aanbieden aan de Key User.
10. Inactieve account (meer dan 1 jaar niet ingelogd) worden verwijderd. Hiervan wordt opnieuw melding gemaakt bij de Key User.

VASTGESTELD DOOR DE VEILIGHEIDSDIRECTIE VAN DE VEILIGHEIDSREGIO HOLLANDS MIDDEN – 16 FEBRUARI 2015