CodeSprinter
Innovating today, shaping tomorrow

Kwetsbaarhedenbeleid

Versie 1.0 · 2026

www.codesprinter.nl

DOCUMENT

Type · Beleidsdocument
Versie · 1.0 (2026)
Opgesteld door · CodeSprinter

CODESPRINTER

Kwikstaartlaan 42
3704 GS Zeist
Nederland

CONTACT

info@codesprinter.nl
www.codesprinter.nl
Noodnummer: 085 - 369 - 7644

GEGEVENS

KVK 94394768
BTW NL005081056B55

01 Inleiding en reikwijdte

02 Identificatie van kwetsbaarheden

03 Beoordeling en classificatie naar ernst

04 Doorlooptijden voor herstel per ernst

05 Patchen en updaten

06 Verantwoord melden van kwetsbaarheden door derden

07 Registratie

08 Verantwoordelijkheden opdrachtgever

09 Evaluatie

HOOFDSTUK 1

Inleiding en reikwijdte

Doel van dit beleid

Dit Kwetsbaarhedenbeleid beschrijft de wijze waarop CodeSprinter omgaat met beveiligingskwetsbaarheden in de systemen, applicaties en softwarecomponenten die zij beheert of ontwikkelt voor opdrachtgevers. Het beleid legt vast hoe kwetsbaarheden worden geïdentificeerd, beoordeeld, geprioriteerd en verholpen, en hoe derden een gevonden kwetsbaarheid op een verantwoorde manier kunnen melden.

Een kwetsbaarheid is een zwakheid in software, configuratie of ontwerp die door een aanvaller kan worden misbruikt om ongeautoriseerde toegang te verkrijgen, gegevens te manipuleren of de werking van een systeem te verstoren. Tijdige identificatie en beheersing van kwetsbaarheden is een essentieel onderdeel van de beveiligingsaanpak van CodeSprinter.

Reikwijdte

Dit beleid is van toepassing op:

- besturingssystemen en serverconfiguraties die CodeSprinter beheert ten behoeve van opdrachtgevers;
- webapplicaties en softwareoplossingen die CodeSprinter ontwikkelt of beheert;
- softwareafhankelijkheden (third-party bibliotheken, frameworks, pakketten) die deel uitmaken van de beheerde applicaties;
- de serverhardware, het besturingssysteem en de infrastructurele componenten die CodeSprinter in eigen beheer heeft, alsmede de diensten van ingeschakelde leveranciers.

Dit beleid is niet van toepassing op systemen of software die volledig buiten de beheerscope van CodeSprinter vallen, tenzij hierover aanvullende afspraken zijn gemaakt in de Softwarebeheer-overeenkomst of de Managed Hosting SLA.

Samenhang met andere documenten

Dit beleid dient in samenhang gelezen te worden met de volgende documenten uit de CodeSprinter Document Suite:

- **Technische en Organisatorische Maatregelen (TOM):** beschrijft de bredere beveiligingsmaatregelen waarvan kwetsbaarhedenbeheer onderdeel uitmaakt (zie Hoofdstuk 8

van de TOM).

- **Softwarebeheer-overeenkomst:** bevat de contractuele afspraken over het uitvoeren van beveiligingsupdates en patchbeheer.
- **Managed Hosting SLA:** regelt de beschikbaarheidsverplichtingen en onderhoudsvensters waarbinnen patches kunnen worden doorgevoerd.
- **Security & Privacy Statement:** beschrijft de bredere beveiligings- en privacyaanpak van CodeSprinter op openbaar niveau.
- **Incident- en datalekprocedure:** is van toepassing zodra een kwetsbaarheid is uitgebuit en een beveiligingsincident of datalek is opgetreden.

HOOFDSTUK 2

Identificatie van kwetsbaarheden

Geautomatiseerde dependency-scans

CodeSprinter maakt gebruik van geautomatiseerde hulpmiddelen om kwetsbaarheden in softwareafhankelijkheden (bibliotheken, pakketten en frameworks) te detecteren. Ingezette scans omvatten Dependabot, dat de repositories doorlopend controleert op kwetsbare afhankelijkheden, aangevuld met npm audit als onderdeel van de CI-pipeline. Deze scans worden uitgevoerd:

- automatisch bij elke nieuwe build of deploy, voor zover de gebruikte tooling dit ondersteunt;
- handmatig bij het bijwerken van een afhankelijkheid of bij het integreren van een nieuw pakket;
- periodiek op de bestaande codebase, met een minimale frequentie van eenmaal per maand.

De uitkomsten van de scans worden beoordeeld op relevantie en ernst en worden, waar nodig, omgezet in een herstelactie.

Beveiligingsmeldingen van leveranciers en projecten

CodeSprinter volgt actief de beveiligingsmeldingen van leveranciers en open-sourceprojecten waarvan de beheerde applicaties afhankelijk zijn. Dit omvat:

- beveiligingsadviezen (security advisories) van de leveranciers van gebruikte besturingssystemen, databases en runtimeomgevingen;
- meldingen via de publieke kwetsbaarheidsdatabases, waaronder de National Vulnerability Database (NVD) en de Common Vulnerabilities and Exposures (CVE)-lijst;
- beveiligingsmeldingen via de officiële kanalen van gebruikte open-sourceframeworks en -bibliotheken;
- relevante bulletins van het Nationaal Cyber Security Centrum (NCSC) van de Nederlandse overheid.

Updates en patchmeldingen volgen

Voor elk systeem en elke softwarecomponent die CodeSprinter beheert, houdt CodeSprinter bij welke versie in gebruik is en of er nieuwere, veiligere versies beschikbaar zijn. Hiervoor worden, afhankelijk van de omgeving, de volgende methoden ingezet:

- automatische installatie van en meldingen over beveiligingsupdates van het besturingssysteem via unattended-upgrades;
- periodieke handmatige controle van de releasenotities en changelogs van kritieke componenten;
- meldingen via geabonneerde beveiligingslijsten of RSS-feeds van relevante leveranciers.

Eigen beveiligingstests

Naast passieve monitoring voert CodeSprinter periodiek actieve controles uit op beheerde systemen en applicaties, waaronder:

- periodieke kwetsbaarheidsscans op serverniveau, met een minimale frequentie van eenmaal per maand;
- handmatige beoordeling van beveiligingskritieke configuraties (toegang, TLS, firewallregels) bij wezenlijke wijzigingen in de omgeving;
- beoordeling van applicatiecode op beveiligingsrisico's als onderdeel van het ontwikkelproces, conform de Secure Development Lifecycle.

HOOFDSTUK 3

Beoordeling en classificatie naar ernst

Classificatiemethodiek

Elke geïdentificeerde kwetsbaarheid wordt beoordeeld op ernst voordat een herstelactie wordt bepaald. CodeSprinter hanteert hierbij de classificatie op basis van het Common Vulnerability Scoring System (CVSS), aangevuld met een contextbeoordeling die rekening houdt met:

- de daadwerkelijke blootstelling van het getroffen systeem of de getroffen component (intern versus extern bereikbaar);
- de aanwezigheid van een bekende, publiek beschikbare exploit;
- de gevoeligheid van de gegevens die de getroffen component verwerkt of waartoe zij toegang heeft;
- de waarschijnlijkheid van misbruik gezien de actuele dreigingsomgeving.

Classificatieniveaus

ERNSTNIVEAUS KWETSBAARHEDEN

CodeSprinter hanteert vier classificatieniveaus. Bij twijfel over de juiste classificatie wordt de hogere klasse aangehouden totdat aanvullend onderzoek uitsluitsel geeft.

Kritiek	Een kwetsbaarheid met een CVSS-score van 9,0 of hoger, of een kwetsbaarheid met een lagere score die door de contextbeoordeling als kritiek wordt aangemerkt. Directe, realistische dreiging van misbruik met ernstige gevolgen: volledige compromittering van een systeem, ongeautoriseerde toegang tot persoonsgegevens of diensten, of volledige uitval van een productieomgeving.
Hoog	Een kwetsbaarheid met een CVSS-score van 7,0 tot 8,9, of een kwetsbaarheid met een lagere score die door de contextbeoordeling als hoog wordt aangemerkt. Aanzienlijk risico op misbruik met significante impact op de vertrouwelijkheid, integriteit of beschikbaarheid van systemen of gegevens.
Middel	Een kwetsbaarheid met een CVSS-score van 4,0 tot 6,9. Beperkt of indirect risico; misbruik vereist doorgaans aanvullende voorwaarden, zoals reeds bestaande (beperkte) toegang, of de impact is beperkt in omvang.
Laag	Een kwetsbaarheid met een CVSS-score van 0,1 tot 3,9. Minimale directe dreiging; mogelijk informatief van aard, of misbruik is slechts theoretisch. Herstel wordt meegenomen in regulier onderhoud.

Contextbeoordeling en bijstelling

Een CVSS-basisscore is een generieke maatstaf die geen rekening houdt met de specifieke inzetomgeving. CodeSprinter past de classificatie aan op basis van de contextuele factoren die hierboven zijn beschreven. Een kwetsbaarheid met een middel-score kan door contextbeoordeling worden opgewaardeerd naar hoog wanneer:

- de getroffen component persoonsgegevens van de opdrachtgever verwerkt;
- de kwetsbaarheid aanwezig is in een extern bereikbaar deel van de applicatie;
- er een publiek bekende exploit beschikbaar is.

Bijgestelde classificaties worden gedocumenteerd in het kwetsbaarhedenregister (zie Hoofdstuk 7), inclusief de motivatie voor de bijstelling.

HOOFDSTUK 4

Doorlooptijden voor herstel per ernst

Uitgangspunten

CodeSprinter stelt concrete doorlooptijden vast voor het verhelpen van kwetsbaarheden. Deze termijnen zijn realistisch gekalibreerd: ze houden rekening met de beschikbare capaciteit, de noodzaak van testen voor productiedeploy, en het vermijden van ondoordachte haastpatches die nieuwe problemen introduceren.

De termijnen gaan in op het moment dat een kwetsbaarheid is geïdentificeerd en geclassificeerd, niet op het moment van eerste ontdekking via een externe bron.

Hersteltermijnen per ernstniveau

- **Kritiek:** herstel of afdoende mitigerende maatregel binnen 48 uur na classificatie. Indien een definitief herstel technisch niet binnen deze termijn haalbaar is (bijv. omdat de leverancier nog geen patch heeft uitgebracht), treft CodeSprinter zo snel mogelijk een tijdelijke mitigerende maatregel (zoals het uitschakelen of isoleren van de getroffen component) en informeert CodeSprinter de opdrachtgever hierover.
- **Hoog:** herstel binnen 7 kalenderdagen na classificatie.
- **Middel:** herstel binnen 30 kalenderdagen na classificatie, of meegenomen in het eerstvolgende geplande onderhoudsvenster dat binnen deze termijn valt.
- **Laag:** herstel binnen 90 kalenderdagen na classificatie, of meegenomen in een reguliere onderhoudsronde.

Afwijking van termijnen

In de volgende situaties kan de hersteldeadline niet worden gehaald:

- de leverancier van het getroffen component heeft nog geen beveiligingspatch uitgebracht;
- het uitvoeren van de patch vereist uitgebreid testen of een geplande onderhoudsperiode om ongewenste uitval te voorkomen;
- de kwetsbaarheid bevindt zich in een component dat technisch of contractueel buiten de beheerscope van CodeSprinter valt.

In al deze gevallen documenteert CodeSprinter de reden van de vertraging en de getroffen mitigerende maatregelen in het kwetsbaarhedenregister. Bij kritieke en hoge kwetsbaarheden informeert CodeSprinter de opdrachtgever actief over de vertraging en de tijdelijke maatregelen, zonder te wachten op een verzoek van de opdrachtgever.

Beschikbaarheid van de opdrachtgever

Voor sommige patches (met name op applicatieniveau of voor updates die functies of interface-elementen kunnen beïnvloeden) is medewerking of een akkoord van de opdrachtgever vereist. In die gevallen informeert CodeSprinter de opdrachtgever zo snel mogelijk en geeft daarbij een duidelijke toelichting op de urgentie. Indien de opdrachtgever een noodzakelijke patch vertraagt of weigert, is de termijnoverschrijding voor rekening van de opdrachtgever (zie ook Hoofdstuk 8).

HOOFDSTUK 5

Patchen en updaten

Testprocedure voor patches

Beveiligingsupdates worden, tenzij de situatie acute directe uitrol vereist (bij kritieke kwetsbaarheden zonder beschikbare mitigatie), eerst geïnstalleerd in een test- of acceptatieomgeving. Hiermee wordt gecontroleerd dat:

- de patch correct werkt en de kwetsbaarheid aantoonbaar verhelpt;
- de patch geen onvoorziene functionaliteitsbreuk introduceert in de applicatie;
- de patch compatibel is met de overige componenten van de omgeving.

De testprocedure is beschreven in de Softwarebeheer-overeenkomst. Voor kritieke kwetsbaarheden waarbij directe productiedeploy noodzakelijk is, wordt de test zo beknopt maar zo grondig mogelijk uitgevoerd, gevolgd door versterkte monitoring na uitrol.

Onderhoudsvensters

Patches worden bij voorkeur uitgerold binnen de overeengekomen onderhoudsvensters zoals vastgelegd in de Managed Hosting SLA of de Softwarebeheer-overeenkomst. Voor kritieke en hoge kwetsbaarheden kan CodeSprinter, na overleg met de opdrachtgever of bij directe dreiging, afwijken van het reguliere onderhoudsvenster en een urgente patch uitrollen buiten de geplande tijdsblokken.

End-of-life componenten

Software, bibliotheken en besturingssystemen die geen beveiligingsupdates meer ontvangen (end-of-life of end-of-support) worden niet ingezet in productieomgevingen die persoonsgegevens verwerken. Wanneer een component de end-of-life-status bereikt, adviseert CodeSprinter de opdrachtgever tijdig over de noodzaak van vervanging of upgrade. De planning en kosten van een dergelijke vervanging vallen buiten het reguliere patchbeheer en worden als meerwerk behandeld conform de Softwarebeheer-overeenkomst.

Documentatie en terugkoppeling

Na uitvoering van een beveiligingsupdate of patch worden de volgende gegevens vastgelegd in het kwetsbaarhedenregister (zie Hoofdstuk 7):

- de geïdentificeerde kwetsbaarheid (inclusief CVE-referentie indien beschikbaar);
- de getroffen component en het versienummer vóór en na de patch;
- de datum van uitrol in test- en productieomgeving;
- de naam van degene die de patch namens CodeSprinter heeft uitgevoerd;
- eventuele bijzonderheden of afwijkingen van de standaard procedure.

De opdrachtgever ontvangt op verzoek een overzicht van uitgevoerde beveiligingsupdates over de afgelopen periode.

HOOFDSTUK 6

Verantwoord melden van kwetsbaarheden door derden

Coordinated Vulnerability Disclosure

CodeSprinter hecht waarde aan de inzet van beveiligingsonderzoekers, ethische hackers en andere derden die kwetsbaarheden in de systemen en applicaties van CodeSprinter of haar opdrachtgevers ontdekken en op een verantwoorde wijze melden. CodeSprinter hanteert hiervoor een regeling voor gecoördineerde kwetsbaarheidsonthulling (Coordinated Vulnerability Disclosure, CVD), ook bekend als responsible disclosure.

Het doel van deze regeling is te zorgen dat kwetsbaarheden zo snel mogelijk worden verholpen zonder dat zij voortijdig publiek worden gemaakt op een wijze die misbruik in de hand werkt.

Meldpunt en contactwijze

Kwetsbaarheden kunnen worden gemeld via:

- **E-mail:** security@codesprinter.net (vermeld "CVD" of "Responsible Disclosure" in de onderwerpregel)
- **Versleuteling:** indien de melder gebruik wenst te maken van PGP-versleuteling voor de melding, kan het publieke sleutelblok worden opgevraagd via hetzelfde e-mailadres.

CodeSprinter bevestigt de ontvangst van een melding binnen 3 werkdagen en streeft ernaar de melder binnen 10 werkdagen te informeren over de initiële beoordeling van de melding.

Wat een verantwoorde melding inhoudt

Een melding wordt als verantwoord beschouwd indien de melder:

- de kwetsbaarheid uitsluitend heeft onderzocht voor zover nodig om het bestaan ervan aan te tonen;
- geen misbruik heeft gemaakt van de kwetsbaarheid, zoals het inzien, kopiëren, aanpassen of verwijderen van gegevens, of het verstoren van de dienstverlening;
- de kwetsbaarheid niet heeft gedeeld met derden totdat CodeSprinter de gelegenheid heeft gehad om het probleem te verhelpen;

- geen gebruik heeft gemaakt van social engineering, phishing, brute-force aanvallen, of andere aanvalsmethoden die niet strikt noodzakelijk zijn voor de demonstratie van de kwetsbaarheid;
- de melding zo spoedig mogelijk heeft gedaan na ontdekking van de kwetsbaarheid;
- de melding indient in het Nederlands of Engels via het in dit hoofdstuk genoemde meldpunt.

Wat niet is toegestaan

De volgende handelingen vallen buiten de reikwijdte van de responsible disclosure-regeling en kunnen aanleiding geven tot juridische stappen, ongeacht de bedoeling van de melder:

- het installeren van malware, backdoors of andere schadelijke software;
- het wijzigen of vernietigen van gegevens;
- het doorsturen, publiceren of voor andere doeleinden gebruiken van aangetroffen gegevens van opdrachtgevers of betrokkenen;
- het uitvoeren van (D)DoS-aanvallen of vergelijkbare verstoringen;
- het verleiden van medewerkers of contactpersonen via social engineering;
- het melden van kwetsbaarheden in systemen van derden die geen deel uitmaken van de door CodeSprinter beheerde omgeving.

Toezegging van CodeSprinter bij verantwoorde melding

Indien een melder zich houdt aan de hierboven beschreven voorwaarden, zegt CodeSprinter het volgende toe:

- CodeSprinter onderneemt geen juridische stappen op grond van de loutere ontdekking en verantwoorde melding van de kwetsbaarheid.
- CodeSprinter behandelt de melding vertrouwelijk en deelt de persoonsgegevens van de melder niet zonder diens toestemming met derden, tenzij CodeSprinter daartoe wettelijk verplicht is.
- CodeSprinter streeft ernaar de kwetsbaarheid te verhelpen conform de hersteltermijnen in Hoofdstuk 4 en informeert de melder over de voortgang.
- Indien de melder dit wenst en CodeSprinter hiermee instemt, kan de melder na herstel van de kwetsbaarheid publiek worden erkend als degene die de melding heeft gedaan (responsible disclosure credit), tenzij anonimiteit gewenst is.

CodeSprinter biedt geen financiële vergoeding (bug bounty) voor kwetsbaarheidsmeldingen, tenzij dit uitdrukkelijk en schriftelijk anders is overeengekomen.

Coördinatie bij kwetsbaarheden in opdrachtgeversystemen

Wanneer een melding betrekking heeft op een applicatie die CodeSprinter beheert namens een opdrachtgever, informeert CodeSprinter de betreffende opdrachtgever zo spoedig mogelijk over de aard van de kwetsbaarheid en de voorgenomen herstelactie. De coördinatie met de melder verloopt via CodeSprinter als aanspreekpunt, tenzij de opdrachtgever uitdrukkelijk verzoekt zelf de communicatie over te nemen.

HOOFDSTUK 7

Registratie

Kwetsbaarhedenregister

CodeSprinter houdt een intern kwetsbaarhedenregister bij van alle geïdentificeerde kwetsbaarheden die zijn beoordeeld als middel of hoger, alsmede van verantwoorde meldingen door derden. Het register dient als aantoonbaar bewijs van het gevoerde kwetsbaarhedenbeheer en als verantwoordingsinstrument richting opdrachtgevers en, indien van toepassing, toezichthoudende instanties.

Per kwetsbaarheid worden in het register ten minste de volgende gegevens vastgelegd:

- **Identificatie:** unieke registratie-ID, datum van identificatie en bron (geautomatiseerde scan, leveranciersbulletin, eigen test of melding door derde).
- **Beschrijving:** omschrijving van de kwetsbaarheid, de getroffen component(en) en versie(s), en de CVE-referentie of equivalente referentie indien beschikbaar.
- **Classificatie:** ernstniveau (kritiek/hoog/middel/laag), CVSS-score indien beschikbaar, en de motivatie bij bijgestelde classificatie.
- **Status:** huidig herstelstatus (open, in behandeling, gemitigeerd, gesloten).
- **Herstelactie:** beschrijving van de uitgevoerde of geplande maatregel, de datum van uitrol in test en productie, en de uitvoerder.
- **Opdrachtgever:** indien van toepassing, de opdrachtgever wiens systeem de kwetsbaarheid betreft.
- **Melding aan opdrachtgever:** datum en wijze van informeren van de opdrachtgever, indien van toepassing.

Bewaring van het register

Het kwetsbaarhedenregister wordt bewaard gedurende een periode van minimaal 3 jaar na afsluiting van de betreffende registratie. Het register is beschikbaar voor inzage door de opdrachtgever op verzoek, voor zover de registraties betrekking hebben op diens systemen. CodeSprinter verstrekt op verzoek een overzicht van afgehandelde kwetsbaarheden over een specificeerde periode.

Relatie met het incidentregister

Indien een kwetsbaarheid wordt uitgebuit en leidt tot een beveiligingsincident of datalek, wordt naast de registratie in het kwetsbaarhedenregister ook een vermelding opgenomen in het incidentregister conform de Incident- en datalekprocedure. Beide registraties verwijzen naar elkaar via de registratie-ID.

HOOFDSTUK 8

Verantwoordelijkheden opdrachtgever

Medewerking bij patchbeheer

Effectief kwetsbaarhedenbeheer vereist medewerking van de opdrachtgever. De opdrachtgever is verantwoordelijk voor:

- het tijdig verlenen van toestemming voor de uitvoering van beveiligingsupdates die invloed kunnen hebben op de beschikbaarheid of het gedrag van de applicatie;
- het beschikbaar stellen van een testomgeving of acceptatieomgeving waarin CodeSprinter patches kan valideren voorafgaand aan productiedeploy, indien de aard van de applicatie dit vereist;
- het tijdig reageren op urgente informatieverzoeken van CodeSprinter bij kritieke of hoge kwetsbaarheden;
- het beschikbaar zijn voor overleg buiten de reguliere kantooruren bij acute beveiligingsincidenten die voortvloeien uit een ernstige kwetsbaarheid.

Beveiliging buiten de beheerscope

De opdrachtgever is zelf verantwoordelijk voor de beveiliging van systemen, applicaties en gegevens die buiten de beheerscope van CodeSprinter vallen, zoals:

- door de opdrachtgever zelf beheerde systemen, accounts of integraties van derden;
- wachtwoorden en toegangsgegevens die de opdrachtgever beheert voor toegang tot de applicatie of het beheerpaneel;
- wijzigingen die de opdrachtgever of een door de opdrachtgever ingeschakelde derde heeft aangebracht aan de applicatie buiten CodeSprinter om.

Kwetsbaarheden die zijn ontstaan als gevolg van handelingen van de opdrachtgever of ingeschakelde derden buiten de beheerscope van CodeSprinter, vallen niet onder de hersteltermijnen van dit beleid en worden, indien herstel gewenst is, behandeld als meerwerk conform de Softwarebeheer-overeenkomst.

Informatieplicht opdrachtgever

De opdrachtgever is verplicht CodeSprinter onverwijld te informeren zodra hij kennis krijgt van een kwetsbaarheid, beveiligingsincident of verdachte activiteit die betrekking heeft op de door CodeSprinter beheerde systemen of applicaties. Vroegtijdige signalering door de opdrachtgever kan de herstelsnelheid aanzienlijk vergroten.

Instructies voor veilig gebruik

De opdrachtgever is verantwoordelijk voor het veilig gebruik van de applicatie door zijn eigen medewerkers en gebruikers, waaronder het hanteren van sterke wachtwoorden, het gebruik van meervoudige authenticatie waar aangeboden, en het tijdig melden van verdachte activiteiten aan CodeSprinter.

HOOFDSTUK 9

Evaluatie

Periodieke beoordeling van het beleid

CodeSprinter beoordeelt dit Kwetsbaarhedenbeleid periodiek op actualiteit, volledigheid en doeltreffendheid. De evaluatie vindt minimaal eenmaal per jaar plaats en in elk geval na:

- een beveiligingsincident waarbij een niet of te laat gepatchte kwetsbaarheid een rol heeft gespeeld;
- een wezenlijke wijziging in de gebruikte technologiestack, de inzetomgeving of de beheerscope;
- een significante wijziging in de dreigingsomgeving of de stand van de techniek op het gebied van kwetsbaarhedenbeheer;
- een relevante wijziging in wet- of regelgeving die van invloed is op de vereisten voor kwetsbaarhedenbeheer.

Leerproces na incidenten en meldingen

Na afhandeling van een kritieke of hoge kwetsbaarheid, en na verwerking van een verantwoorde melding van een derde, evalueert CodeSprinter of de huidige identificatie-, classificatie- en herstelprocedures afdoende hebben gefunctioneerd. Leerpunten worden vastgelegd en verwerkt in het beleid of de ondersteunende procedures.

Versioning en communicatie

Dit beleid wordt bij elke wezenlijke wijziging voorzien van een nieuw versienummer en een herzieningsdatum. Opdrachtgevers die een Softwarebeheer-overeenkomst of Managed Hosting SLA met CodeSprinter hebben gesloten, worden geïnformeerd over nieuwe versies die van invloed kunnen zijn op de overeengekomen werkwijze. De meest actuele versie van dit beleid is beschikbaar via info@codesprinter.nl.