Nederlandse
Ski Vereniging

INFORMATIEBEVEILIGINGSBELEID NSkiV

Informatiebeveiligingsbeleid NSkiV			
Classificatie		intern	
Opgesteld door		S.M. Vierhout	
Eigenaar		S.M. Vierhout	
Vastgesteld op 8 september 2026			
Versie	Wijzigingen	Datum goedkeuring	Goedgekeurd door
1.0			

Nederlandse Ski Vereniging

Inhoudsopgave

1 Belangrijke begrippen 3
2 Inleiding 4
2.1 Doelstelling 5
2.2 Toepassingsgebied 5
2.3 Wet- en regelgeving 5
2.4 Aanvullende afspraken en documenten 5
2.5 Inwerkingtreding en evaluatie 6
3 Uitgangspunten informatiebeveiliging 6
4 Verantwoordelijkheden 7
4.1 Bestuur 7
4.2 Aanspreekpunt informatiebeveiliging 7
4.3 Medewerkers en vrijwilligers 7
4.4 Gebruik van externe partijen 7
5 Informatiebeveiligingsmaatregelen 8
5.1 Basismaatregelen informatiebeveiliging 8
5.2 Aanvullende maatregelen bij verhoogde risico's 9
5.3 Beveiliging bij wijzigingen en vernieuwingen 10
5.4 Ondersteuning en expertise 10
6 Beheer van informatiebeveiligingsincidenten 10
6.1 Melden van incidenten 10
6.2 Beoordeling en classificatie 10
6.3 Afhandeling en respons 11
6.4 Herstel van systemen en gegevens 11
6.5 Evaluatie en leren van incidenten 11
6.6 Registratie en monitoring 11
6.7 Communicatie en meldplicht 11
7 Beheer van het beleid 12

1 Belangrijke begrippen

Binnen dit informatiebeveiligingsbeleid wordt een aantal begrippen gebruikt die hieronder worden toegelicht. Deze begrippen helpen om het beleid eenduidig te kunnen interpreteren en toepassen binnen de organisatie.

Informatie
Alle gegevens die binnen de organisatie worden gebruikt of verwerkt. Dit kan gaan om digitale gegevens in systemen zoals ledenadministratie of CMSS, maar ook om e-mails, documenten en papieren dossiers.

Informatiebeveiliging
Het geheel van maatregelen en afspraken dat erop gericht is om informatie te beschermen tegen verlies, misbruik of onbevoegde toegang. Daarbij staat centraal dat informatie vertrouwelijk, correct en beschikbaar blijft.

Vertrouwelijkheid
Het principe dat informatie alleen toegankelijk is voor personen die daarvoor geautoriseerd zijn. Dit is met name van belang bij gevoelige informatie, zoals gegevens over meldingen of incidenten.

Integriteit
Het principe dat informatie correct, volledig en actueel is en niet ongewenst wordt gewijzigd.

Beschikbaarheid
Het principe dat informatie (en de systemen waarin informatie is opgeslagen) beschikbaar is op het moment dat deze benodigd is voor de uitvoering van werkzaamheden.

Bijzondere persoonsgegevens
Categorieën van persoonsgegevens die door hun aard bijzonder gevoelig zijn, als bedoeld in art. 9 AVG. Voorbeelden zijn gegevens die iets zeggen over iemands gezondheid, ras, godsdienst of seksuele leven, maar ook een lidmaatschap van een vakvereniging of politieke partij.

Strafrechtelijke persoonsgegevens
Persoonsgegevens die betrekking hebben op strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen, zoals bedoeld in artikel 10 AVG en artikel 1 UAVG, waaronder gegevens die zodanig concrete feiten en omstandigheden bevatten dat zij een bewezenverklaring van een strafbaar feit in de zin van artikel 350 Sv kunnen dragen. Er gelden speciale regels voor het verwerken van strafrechtelijke persoonsgegevens.

Gevoelige persoonsgegevens
Gevoelige persoonsgegevens zijn persoonsgegevens waarvan misbruik, verlies of ongeautoriseerde toegang een grotere impact kan hebben op de privacy of belangen van een persoon dan bij gewone persoonsgegevens. In de AVG staat expliciet benoemd dat bijzondere persoonsgegevens en strafrechtelijke gegevens zó gevoelig zijn dat daarvoor speciale regels nodig zijn. Er zijn echter ook gegevens die niet expliciet in de AVG zijn benoemd als gevoelig, maar die wel een grotere impact hebben op iemands privacy dan gewone persoonsgegevens. Persoonsgegevens die als privacygevoelig worden beschouwd, zijn bijvoorbeeld locatiegegevens, financiële gegevens en het Burgerservicenummer (BSN).

Beveiligingsincident
Een gebeurtenis waarbij de vertrouwelijkheid, integriteit of beschikbaarheid van informatie (mogelijk) is aangetast. Dit kan bijvoorbeeld gaan om een datalek, verlies van gegevens of ongeautoriseerde toegang tot systemen.

Toegangsbeheer
Het geheel van maatregelen waarmee wordt bepaald wie toegang heeft tot welke informatie en systemen. Binnen de organisatie wordt hierbij gewerkt volgens het principe dat toegang alleen wordt verleend wanneer dit noodzakelijk is voor de uitvoering van werkzaamheden.

Need-to-knowprincipe
Het uitgangspunt dat medewerkers alleen toegang hebben tot die informatie die zij nodig hebben voor hun rol. Dit principe is met name van belang bij gevoelige gegevens.

Logging
Het vastleggen van activiteiten binnen systemen, zodat achteraf kan worden gecontroleerd wie toegang heeft gehad tot informatie en welke handelingen zijn uitgevoerd.

2 Inleiding
Binnen de Nederlandse Ski Vereniging (hierna: “NSkiV”) wordt gewerkt met informatie over leden, sporters, vrijwilligers en medewerkers. Daarnaast kan de organisatie, bijvoorbeeld via het gebruik van CMSS, betrokken zijn bij het verwerken van gevoelige gegevens over meldingen en strafrechtelijke persoonsgegevens bij integriteitsschendingen binnen de sport. Dit soort informatie vraagt om een verhoogd niveau van zorgvuldigheid en bescherming. In dit informatiebeveiligingsbeleid beschrijven wij hoe wij als organisatie omgaan met informatie en welke uitgangspunten wij hanteren om deze te beschermen. Het beleid sluit aan bij onze verantwoordelijkheid om een veilige sportomgeving te bieden. Leden en betrokkenen moeten er in dit kader op kunnen vertrouwen dat hun (gevoelige) gegevens passend worden beschermd.

2.1 Doelstelling

Het doel van dit beleid is het vaststellen van uitgangspunten, regels en maatregelen voor informatiebeveiliging om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen. Dit betekent dat informatie alleen toegankelijk is voor bevoegde personen, correct en volledig blijft en beschikbaar is wanneer dat nodig is. Het beleid helpt om risico's zoals datalekken, misbruik of ongeautoriseerde toegang te beperken en biedt medewerkers en vrijwilligers handvatten voor veilig werken.

2.2 Toepassingsgebied

Dit beleid is van toepassing op alle informatie en informatiesystemen die binnen de NSkiV worden gebruikt, ongeacht de vorm waarin de informatie zich bevindt. Dit omvat onder andere digitale systemen, applicaties, e-mail, documenten en papieren dossiers.

Het beleid geldt voor alle personen die werkzaamheden verrichten voor of namens de organisatie, waaronder medewerkers, vrijwilligers, bestuursleden en externe partijen die toegang hebben tot systemen of informatie.

Voor processen waarbij sprake is van verhoogde risico's, zoals de verwerking van bijzondere of strafrechtelijke gegevens, gelden aanvullende beveiligingsmaatregelen. Deze kaders worden tevens in dit document beschreven.

2.3 Wet- en regelgeving

De NSkiV handelt in overeenstemming met de geldende wet- en regelgeving op het gebied van informatiebeveiliging en privacy, waaronder de Algemene Verordening Gegevensbescherming (AVG) en de ePrivacy directive. In het bijzonder wordt invulling gegeven aan de verplichting om passende technische en organisatorische maatregelen te treffen (artikel 32 AVG). Daarbij beoordelen wij vooraf de risico's van gegevensverwerkingen om passende maatregelen te kunnen treffen.

Bij de inrichting van informatiebeveiliging wordt waar mogelijk aangesloten bij gangbare normen en richtlijnen, zoals ISO 27001 en/of de Baseline Informatiebeveiliging Overheid (BIO). Bij de toepassing van deze maatregelen wordt expliciet rekening gehouden met de omvang en aard van de organisatie: op basis van het proportionaliteitsbeginsel wordt bekeken wat passend en haalbaar is.

2.4 Aanvullende afspraken en documenten

Dit informatiebeveiligingsbeleid vormt het kader voor de manier waarop de NSkiV omgaat met informatiebeveiliging.

Het beleid hangt samen met het Privacybeleid (link toevoegen) van de NSkiV, waarin wordt ingegaan op de verwerking van persoonsgegevens.

2.5 Inwerkingtreding en evaluatie

Dit informatiebeveiligingsbeleid treedt in werking na vaststelling door het Bestuur. Het beleid wordt periodiek geëvalueerd en waar nodig aangepast, bijvoorbeeld naar aanleiding van wijzigingen in wetgeving, technologische ontwikkelingen of beveiligingsincidenten.

3 Uitgangspunten informatiebeveiliging

Binnen de NSkiV gaan wij zorgvuldig om met informatie. Dit geldt voor persoonsgegevens, maar ook voor andere vertrouwelijke of bedrijfsgevoelige informatie. De onderstaande uitgangspunten vormen de basis voor hoe wij binnen de organisatie omgaan met informatie.

Noodzakelijkheid en doelgericht gebruik
Wij gebruiken en verwerken alleen informatie die nodig is voor onze werkzaamheden en voor een duidelijk en vooraf bepaald doel. Informatie wordt niet gebruikt voor andere doeleinden dan waarvoor deze is verzameld, tenzij dit passend en toegestaan is.

Zorgvuldigheid en betrouwbaarheid
Wij gaan zorgvuldig om met informatie en zorgen dat deze correct en zo actueel mogelijk blijft. Onjuistheden worden waar mogelijk hersteld.

Beveiliging als basisprincipe
Wij beschermen informatie tegen verlies, misbruik en onbevoegde toegang. Informatiebeveiliging is een vast onderdeel van onze dagelijkse werkzaamheden en wordt meegenomen in de inrichting en het gebruik van systemen en processen.

Beperkte toegang en vertrouwelijkheid
Toegang tot informatie is beperkt tot personen die deze nodig hebben voor hun werkzaamheden. Wij gaan vertrouwelijk om met informatie en zijn terughoudend in het delen daarvan.

Bewust en verantwoord handelen
Medewerkers, vrijwilligers en andere betrokkenen zijn zich bewust van het belang van informatiebeveiliging en handelen hiernaar. Bij twijfel over het gebruik of delen van informatie wordt altijd zorgvuldig gehandeld en zo nodig advies gevraagd.

Beheer en opschoning van informatie
Informatie wordt niet langer bewaard dan nodig is voor het doel waarvoor deze is verzameld. Wanneer informatie niet meer nodig is, wordt deze verwijderd of op een passende manier gearchiveerd.

Transparantie en communicatie
Wij zijn transparant en melden (mogelijke) beveiligingsincidenten en datalekken zo snel mogelijk, zodat passende maatregelen genomen kunnen worden en schade beperkt blijft.

4 Verantwoordelijkheden
Binnen de NSkiV is iedereen verantwoordelijk voor een zorgvuldige omgang met informatie en het naleven van afspraken rondom informatiebeveiliging. Om dit goed te organiseren zijn de volgende rollen en verantwoordelijkheden afgesproken.

4.1 Bestuur
Het Bestuur is eindverantwoordelijk voor informatiebeveiliging binnen de organisatie. Het Bestuur zorgt ervoor dat:
- dit informatiebeveiligingsbeleid wordt vastgesteld en nageleefd;
- informatiebeveiliging onderdeel is van de dagelijkse bedrijfsvoering;
- risico's tijdig worden gesignaleerd en waar nodig maatregelen worden genomen.

4.2 Aanspreekpunt informatiebeveiliging
Binnen de NSkiV is Steven Vierhout, operationeel directeur, aangewezen als aanspreekpunt voor informatiebeveiliging. Het aanspreekpunt:
- ondersteunt medewerkers en vrijwilligers bij vragen over veilig omgaan met informatie;
- houdt overzicht over hoe binnen de organisatie met informatie en systemen wordt omgegaan;
- signaleert risico's en bespreekt deze met het Bestuur.

4.3 Medewerkers en vrijwilligers
Iedereen die werkt voor de NSkiV is verantwoordelijk voor een zorgvuldige omgang met informatie. Dit betekent dat zij:
- informatie alleen gebruiken voor hun werkzaamheden;
- zorgvuldig omgaan met systemen, documenten en gegevens en hun verantwoordelijkheden hierin kennen en toepassen;
- beveiligingsrisico's en incidenten tijdig melden.

4.4 Gebruik van externe partijen
Als de NSkiV samenwerkt met externe partijen die toegang hebben tot systemen of informatie,

maakt zij hierover duidelijke afspraken. Deze afspraken hebben onder andere betrekking op beveiliging, vertrouwelijkheid en het gebruik van informatie. De NSkiV is eindverantwoordelijk voor de beveiliging en vertrouwelijkheid van informatie die bij externe partijen is opgeslagen.

5 Informatiebeveiligingsmaatregelen

Binnen de NSkiV worden passende technische en organisatorische maatregelen genomen om informatie te beschermen. De aard en zwaarte van deze maatregelen sluiten aan bij de risico's die samenhangen met de verwerking van informatie. Dit betekent dat voor reguliere werkzaamheden wordt gewerkt met een set basismaatregelen, en dat waar sprake is van verhoogde risico's aanvullende of zwaardere maatregelen worden getroffen.

5.1 Basismaatregelen informatiebeveiliging

Binnen de organisatie worden in ieder geval de volgende maatregelen toegepast:

Toegangsbeheer en accounts
Toegang tot systemen en informatie is persoonlijk en gekoppeld aan de rol en werkzaamheden van de gebruiker. Het gebruik van gedeelde accounts wordt zoveel mogelijk vermeden. Toegangsrechten worden aangepast bij functiewijzigingen en direct ingetrokken bij uitdiensttreding.

Beveiliging van systemen en apparaten
Systemen en apparaten worden voorzien van actuele beveiligingsupdates en passende beveiligingsmaatregelen. Apparaten worden vergrendeld wanneer deze niet in gebruik zijn.

Gebruik van privé-apparaten
Wanneer privé-apparaten worden gebruikt voor werkzaamheden, wordt zorgvuldig omgegaan met informatie en worden basisbeveiligingsmaatregelen toegepast (zoals een automatische apparaatvergrendeling en het tijdig doorvoeren van de aangeboden updates).

Wachtwoorden en aanvullende beveiliging
Er wordt gebruikgemaakt van sterke wachtwoorden en tweestapsverificatie. Indien tweestapsverificatie bij een specifiek systeem niet wordt ondersteund of niet mogelijk is, wordt bepaald of er additionele maatregelen mogelijk of noodzakelijk zijn.

Veilig gebruik van e-mail en communicatie
Medewerkers en vrijwilligers gaan zorgvuldig om met e-mail en andere communicatiemiddelen. Zij controleren ontvangers en zijn alert op risico's zoals phishing en onveilige links.

Opslag van informatie
Informatie wordt opgeslagen in daarvoor bestemde systemen. Het lokaal opslaan van informatie of het gebruik van onbeveiligde opslaglocaties wordt zoveel mogelijk beperkt.

Delen van informatie
Informatie wordt alleen gedeeld met anderen als dit noodzakelijk is in het kader van de bedrijfsvoering. Informatie wordt gedeeld via passende en veilige middelen.

Fysieke beveiliging
Werkplekken, apparatuur en papieren documenten worden zodanig beheerd dat onbevoegden geen toegang hebben tot informatie. Vertrouwelijke informatie wordt niet onbeheerd achtergelaten.

Back-ups en herstel
Van belangrijke gegevens worden back-ups gemaakt zodat deze kunnen worden hersteld bij incidenten of technische storingen.

Logging
Waar mogelijk wordt logging toegepast om systeemactiviteit inzichtelijk te maken en afwijkingen of misbruik, indien nodig, te kunnen onderzoeken.

Incidenten en datalekken
Beveiligingsincidenten en datalekken worden gemeld en zorgvuldig opgevolgd. Er wordt gekeken naar de oorzaak en waar nodig worden maatregelen genomen om herhaling te voorkomen. Datalekken worden conform het Privacybeleid gemeld bij de Autoriteit Persoonsgegevens.

5.2 Aanvullende maatregelen bij verhoogde risico's
Wanneer sprake is van informatie met een verhoogd risico, zoals bijzondere of gevoelige persoonsgegevens, worden aanvullende maatregelen getroffen. Afhankelijk van de situatie kan dit bijvoorbeeld betekenen dat:
- toegang verder wordt beperkt tot een kleine groep bevoegde personen of dat er functiescheiding wordt toegepast;
- extra beveiligingsmaatregelen worden toegepast, zoals versleuteling of aanvullende authenticatie;
- additionele logging of monitoring wordt ingezet;
- strengere afspraken gelden voor het delen van informatie;
- een aanvullende risicoafweging wordt gemaakt voorafgaand aan de verwerking.

Welke maatregelen nodig zijn, wordt per situatie bepaald.

5.3 Beveiliging bij wijzigingen en vernieuwingen
Bij de invoering van nieuwe systemen, processen of samenwerkingen wordt gekeken naar de gevolgen voor informatiebeveiliging. Waar nodig worden aanvullende maatregelen genomen voordat het nieuwe systeem, proces of de samenwerking wordt ingevoerd.

5.4 Ondersteuning en expertise
Indien binnen de organisatie onvoldoende kennis of capaciteit aanwezig is om passende maatregelen te bepalen of te implementeren, wordt externe expertise ingeschakeld.

6 Beheer van informatiebeveiligingsincidenten
Binnen de NSkiV kunnen zich situaties voordoen waarbij de beveiliging van informatie in het gedrang komt. Het is daarom van groot belang dat de organisatie beschikt over een duidelijke en zorgvuldige werkwijze voor het melden, beoordelen en afhandelen van informatiebeveiligingsincidenten.

Een informatiebeveiligingsincident is iedere gebeurtenis waarbij de vertrouwelijkheid, integriteit of beschikbaarheid van informatie mogelijk is aangetast. Dit kan variëren van relatief eenvoudige situaties, zoals het versturen van een e-mail naar een verkeerde ontvanger, tot meer ernstige incidenten zoals ongeautoriseerde toegang tot systemen of verlies van gevoelige gegevens, waaronder informatie over meldingen of strafrechtelijke gegevens.

6.1 Melden van incidenten
Iedereen die werkt voor of namens de NSkiV is verantwoordelijk voor het tijdig melden van (vermoedens van) informatiebeveiligingsincidenten. Dit geldt ook voor situaties waarin twijfel bestaat over de ernst of aard van een incident. Meldingen worden gedaan bij het aanspreekpunt voor informatiebeveiliging, zodat snel kan worden beoordeeld welke acties nodig zijn.

De organisatie zorgt ervoor dat duidelijk is waar en hoe incidenten gemeld kunnen worden en stimuleert een open meldcultuur waarin medewerkers en vrijwilligers zonder terughoudendheid incidenten kunnen rapporteren.

6.2 Beoordeling en classificatie
Na melding wordt het incident zo spoedig mogelijk beoordeeld. Indien nodig worden direct eerste maatregelen genomen om verdere verspreiding of escalatie te voorkomen, zoals het blokkeren van toegang, het intrekken van rechten of het veiligstellen van systemen en gegevens. Vervolgens wordt het incident inhoudelijk geclassificeerd. Daarbij wordt gekeken naar de aard van het incident, de betrokken gegevens en de mogelijke gevolgen voor betrokkenen en de organisatie. In het bijzonder wordt beoordeeld of sprake is van gevoelige gegevens, zoals strafrechtelijke gegevens of informatie over meldingen.

Op basis van deze beoordeling wordt de ernst en prioriteit van het incident bepaald en vastgesteld welke vervolgstappen nodig zijn. Indien sprake is van een datalek, wordt beoordeeld of melding moet worden gedaan bij de Autoriteit Persoonsgegevens en of betrokkenen moeten worden geïnformeerd, conform de geldende wettelijke verplichtingen.

6.3 Afhandeling en respons

De NSkiV treft passende maatregelen om de gevolgen van het incident te beperken en herhaling op korte termijn te voorkomen. Dit kan bijvoorbeeld betekenen dat toegang tot systemen wordt aangepast, gegevens worden veiliggesteld of dat betrokken partijen worden geïnformeerd. Indien nodig worden aanvullende beveiligingsmaatregelen genomen om verdere schade te voorkomen. Hierbij wordt gehandeld volgens de uitgangspunten uit dit beleid, waarbij zorgvuldigheid, snelheid en proportionaliteit centraal staan.

6.4 Herstel van systemen en gegevens

Na een incident wordt beoordeeld welke systemen en gegevens hersteld moeten worden. De NSkiV zorgt ervoor dat gegevens waar mogelijk worden hersteld en dat de werkzaamheden zo snel mogelijk worden hervat. Hierbij wordt rekening gehouden met de betrouwbaarheid en volledigheid van de herstelde gegevens.

6.5 Evaluatie en leren van incidenten

Na afhandeling van een incident wordt een evaluatie uitgevoerd om de oorzaak en het verloop van het incident te analyseren. Op basis hiervan wordt gekeken naar mogelijke verbeterpunten in processen, systemen of werkwijzen. De uitkomsten van deze evaluatie worden gebruikt om de informatiebeveiliging te versterken en herhaling van vergelijkbare incidenten te voorkomen, bijvoorbeeld door aanpassing van werkwijzen, extra aandacht voor bewustwording of aanvullende technische maatregelen.

6.6 Registratie en monitoring

Informatiebeveiligingsincidenten en de uitkomsten van de uitgevoerde analyse en evaluatie worden vastgelegd, zodat inzicht ontstaat in de aard, frequentie en impact van incidenten. Dit stelt de organisatie in staat om trends te signaleren en gericht verbetermaatregelen te treffen.

6.7 Communicatie en meldplicht

De communicatie over incidenten vindt zorgvuldig plaats en wordt afgestemd op de aard en impact van het incident. Indien nodig worden betrokkenen geïnformeerd op een manier die past bij de situatie en de gevoeligheid van de gegevens.
Wanneer sprake is van een datalek dat gemeld moet worden bij de Autoriteit Persoonsgegevens, wordt dit tijdig en conform de wettelijke eisen uitgevoerd. Indien het incident betrekking heeft op

systemen of verwerkingen waarbij wordt samengewerkt met andere partijen, zoals NOC*NSF, wordt ook met deze partijen afgestemd.



7 Beheer van het beleid

Actualisatie
Wij zorgen ervoor dat dit beleid en de bijbehorende afspraken actueel en passend blijven.
Het beleid wordt:

- minimaal eens per twee jaar beoordeeld, en
- eerder aangepast als er belangrijke veranderingen zijn in de organisatie, wetgeving (zoals de AVG) of werkwijze.

Na wijzigingen wordt het beleid opnieuw vastgesteld.

Uitzonderingen op het beleid
In sommige gevallen kan het nodig zijn om af te wijken van (onderdelen van) dit beleid, bijvoorbeeld door praktische beperkingen of specifieke uitzonderingssituaties.
In dat geval:
- wordt de afwijking vastgelegd, inclusief de reden en eventuele risico's;
- wordt gekeken of aanvullende maatregelen nodig zijn om risico's te beperken.

Uitzonderingen worden periodiek beoordeeld om te bepalen of ze nog van toepassing zijn.