Weerbaarheid en security statement

Inleiding

NHG beschikt over - vaak gevoelige - (persoons)gegevens. Veel van die gegevens zijn afkomstig van onze ketenpartners: geldverstrekkers en hun servicers. Een schending van de beschikbaarheid, integriteit of vertrouwelijkheid van die gegevens of de systemen waarin die worden verwerkt, bijvoorbeeld door fraude, kwaadaardige of foutieve software of een hack, kan verstrekkende gevolgen hebben.

Met een uitgebreide set maatregelen doen we er alles aan om een schending van het recht op privacy van onze klanten, storingen en uitval van onze systemen en financiële of imagoschade bij NHG en haar stakeholders te voorkomen. Dit statement is met name bedoeld om ketenpartners inzicht te geven in de maatregelen die NHG treft, en hen daarmee enige mate van zekerheid te bieden.

Hoofdstuk 1 geeft een generieke omschrijving. In hoofdstuk 2 sommen we de voornaamste concrete maatregelen op.

HOOFDSTUK 1: GENERIEKE OMSCHRIJVING

Context

Wet- en regelgeving

Relevante wet- en regelgeving vormt de kaders. Hierbij zijn met name de 'Algemene verordening gegevensbescherming' (AVG) en de 'Verordening digitale operationele weerbaarheid voor de financiële sector' van belang.

Stakeholders

Bij het bepalen van maatregelen houdt NHG rekening met de belangen van haar stakeholders. Vooral de belangen van de ketenpartners worden hierin gekend. Daarnaast worden ook de belangen van de Raad van Commissarissen, het ministerie van Financiën, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, het ministerie van Volkshuisvesting en Ruimtelijke Ordening en partijen als Vereniging Eigen Huis, de Autoriteit Financiële Markten en De Nederlandsche Bank meegewogen.

Interne ontwikkelingen

NHG is volop in ontwikkeling. Nieuwe processen, producten en ICT-systemen volgen elkaar snel op. De ICT van NHG is grotendeels ondergebracht in de cloud en een groeiend aantal externe bronnen wordt ontsloten of gekoppeld. Al deze ontwikkelingen vragen om aandacht vanuit privacy, security en weerbaarheid.

Dreigingen

De volgende dreigingen vormen input voor de analyses van zwakten en dreigingen (risico's):

1. Cyberdreiging (waar onder hacking, phishing, virussen, ransomware enz.) al dan niet gefinancierd door 'vijandige' staten gericht op financieel gewin, het aanrichten van schade of verkrijgen van (persoons)gegevens.

2. Bewust foutief handelen van een medewerker of leverancier, eveneens gericht op financieel gewin, het aanrichten van schade of verkrijgen van (persoons)gegevens.
3. Onbewust foutief handelen van een medewerker of leverancier dat kan leiden tot foute betalingen of lekken van (persoons)gegevens.
4. Het niet of onvoldoende voldoen aan wet- en regelgeving dat kan leiden tot compliance overtredingen, een schending van de privacy van klanten of medewerkers, boetes en reputatieschade.
5. Onverwachte pieken in verwerkingsbehoeften, fouten in software al dan niet van derden, geopolitieke spanningen en technologische ontwikkelingen die kwaadwillend kunnen worden ingezet zoals quantum computing en artificiële intelligentie kunnen leiden tot allerhande ongewenste gevolgen voor onze systemen en gegevens.

Risicobeheer
NHG heeft een risicomanagementcyclus ingericht volgens het *'three lines of defense'* model. Het hoogst leidinggevende orgaan van NHG, de Raad van Bestuur (RvB), is eindverantwoordelijk voor risicobeheer. In de risicotaxonomie worden risico's beheerd op de vlakken strategisch, financieel, ICT, operationeel, compliance, privacy en security. Risico's worden elke kwartaal gerapporteerd en besproken in het risicocomité waarin de voltallige Raad van Bestuur, het voltallige managementteam en de risicofunctionarissen van NHG zitting hebben. De risicorapportage wordt besproken in de Auditcommissie en gedeeld met de Raad van Commissarissen.

DNB Good practice informatiebeveiliging
Voor een goede borging van (cyber-)security hanteert NHG de 'DNB Good practice informatiebeveiliging'. Daartoe is een securitystrategie en een securitybeleid opgesteld als ook een security architectuur, een risicoanalyse die periodiek wordt herijkt, een verbeterplan en een procedure beveiligingsincidenten. Daarnaast wordt intensief gewerkt aan awareness en kennis, kent NHG een gedegen screeningsproces en worden periodiek zelfbeoordelingen en onafhankelijke beoordelingen uitgevoerd.

Nymity Privacy Management Accountability Framework
Voor de borging van privacy hanteert NHG het 'Nymity Privacy Management Accountability Framework'. Dit framework onderkent 55 technische en organisatorische maatregelen die bij een volwassen implementatie leiden tot een gedegen inrichting en aanpak van privacy.

Proces
Bij de aanpak van risicobeheer, security en privacy volgt NHG een cyclisch proces (*plan-do-check-act*). Op basis van de uitkomst van evaluaties en controles of door nieuwe ontwikkelingen kan het nodig zijn het beleid aan te passen of extra maatregelen te treffen. Ook is het mogelijk dat nieuwe ontwikkelingen, zoals de komst van nieuwe technieken of de introductie van nieuwe bedrijfsprocessen of informatiesystemen, aanleiding geven om het beleid te herzien. Bij het realiseren van verbeteringen volgen we een risico gebaseerde aanpak.

Privacy & Security by design
NHG past *Privacy & Security by Design* toe door te zorgen dat al in de ontwerpfase van nieuwe processen en producten de juiste maatregelen worden geïdentificeerd en borgt dat deze tijdens de gehele levenscyclus worden geïmplementeerd.

Multi layered security, Defense in depth en Zero trust
Alle toepassingen waarin persoonsgegevens van onze klanten en medewerkers worden verwerkt en toepassingen die bedoeld zijn voor financiële transacties zijn beschermd door meerdere beveiligingslagen. Zo wordt naast encryptie en credentials altijd MFA, IP Whitelist of een token toegepast. Toegang tot de bedrijfsdata is alleen mogelijk als de identiteit en het device dat wordt gebruikt voldoet aan de compliance vereisten en netwerkverkeer wordt beveiligd en gelogd.

Voor voorzieningen die wij aan onze ketenpartners aanbieden geldt hetzelfde. Daarop wordt naast encryptie en credentials altijd Multi Factor Authenticatie door middel van een 2-weg certificaat of – bij het portaal – een SMS of app op de telefoon van de gebruiker toegepast. Ook is een Web Application Firewall actief, is monitoring en detectie ingericht en is DDoS bescherming actief.

Due dilligence
NHG is een regieorganisatie op het gebied van ICT: veel ICT-diensten zijn uitbesteed. Bij de selectie van leveranciers stelt NHG hoge eisen aan de leverende organisatie en de te leveren techniek op het gebied van informatiebeveiliging. Binnen het beheer van ICT-risico worden risico's op het vlak van (overeenkomsten met) leveranciers, zoals het risico op een vendor lock-in, tijdens de gehele looptijd van de relatie met de leverancier gemonitord en beheerd.

In de regel zijn de partijen die NHG inzet gerenommeerde en gecertificeerde bedrijven die informatiebeveiliging hoog in het vaandel dragen. Daarnaast hebben we met alle partijen die persoonsgegevens verwerken een verwerkersovereenkomst gesloten waarin ook de meldplicht datalekken is geadresseerd. De datacenters die NHG gebruikt geven een SOC2 of ISAE-rapportage af. Daarnaast is met de IT-leveranciers een Service Level Agreement overeengekomen. Het proces rondom het beheer van de afspraken met leveranciers maakt onderdeel uit van de ISAE 3402 controle van NHG.

Continuïteit
NHG heeft een continuïteitsplan en meerdere plannen voor verschillende noodscenario's. Verantwoordelijkheden en taken van het crisisteam zijn daarin toegewezen. We hebben scenario's uitgewerkt voor de situatie waarin de bedrijfslocatie niet beschikbaar is en voor situaties waarbij bepaalde IT-voorzieningen (tijdelijk) niet beschikbaar zijn. Ook is een procedure aanwezig waarin is beschreven hoe en door wie communicatie over beveiligingsincidenten en datalekken – indien relevant - aan ketenpartners, medewerkers, klanten en publiek en media plaats moet vinden.

Voor IT-voorzieningen is voorzien in back-ups – zowel onsite als offsite - en zijn passende maatregelen voor hoge beschikbaarheid getroffen. Regelmatig testen we of

een back-up kan worden hersteld. Voor de toepassingen die worden gebruikt in de hypotheek-processen van onze ketenpartners, zoals de NHG Toets en het NHG Portaal, is een hoge beschikbaarheid vereist. Met de leveranciers van deze diensten worden Service Level Agreements afgesloten om het beschikbaarheidspercentage van 99,5% te garanderen. Daarvoor is een *fallback* en *failover* ingericht die bij een storing in de primaire availability zone automatisch overgaat naar de secundaire availability zone met maximaal 15 minuten dataverlies. In de praktijk wordt een hoger beschikbaarheidspercentage behaald. Resourcegebruik van deze toepassingen wordt gemonitord en een ruime reservecapaciteit is aanwezig die een eventuele extra verwerkingsbehoefte kan afhandelen.

Controles
NHG voert periodieke interne controles uit op de opzet, het bestaan en de werking van de getroffen maatregelen. We voeren regelmatig technische scans (pentesten) uit op de verschillende diensten die NHG heeft uitbesteed. In deze tests wordt specifiek aandacht besteed aan de scheiding van gegevens van verschillende ketenpartners en de voornaamste dreigingen (OWASP). Periodiek wordt in opdracht van de Raad van Commissarissen een onafhankelijk onderzoek uitgevoerd naar verschillende ICT-, privacy-, en security-domeinen.

Jaarlijks publiceert NHG een ISAE 3402 Assurance-rapport waarbij een externe accountant onafhankelijk de operationele werking test van de interne controles. Het Assurance-rapport kan door stakeholders worden opgevraagd en gaat in op de inrichting van processen en de beoogde beheersdoelstellingen. Hiermee geeft NHG inzicht aan stakeholders in de processen en in de zekerheden die NHG biedt.

HOOFDSTUK 2: CONCRETE MAATREGELEN

In de volgende twee paragrafen is een overzicht opgenomen van de voornaamste door NHG getroffen maatregelen.

Security
- De werkplek (laptop) van alle NHG medewerkers, inclusief tijdelijke krachten en ingehuurd personeel, wordt beschermd door een firewall en antivirus- en antimalware software die continu updates ontvangt van nieuwe kwaadaardige signatures. Updates en securitypatches worden op regelmatige basis, nadat ze zijn getest, geautomatiseerd uitgerold. Daarnaast is de harddrive versleuteld en wordt de werkplek vergrendeld met wachtwoord, pin of facial recognition.
- Toegang met de laptops tot het netwerk is aanvullend afgeschermd met MFA. Door middel van mobile device management worden devices centraal beheerd en kunnen alleen in de netwerkomgeving komen als ze voldoen aan de compliance- en beveiligingsvereisten. Als op een device vermoedelijk een virus, malware of ongewenste software wordt gedetecteerd, wordt onmiddellijk en geautomatiseerd de toegang tot het netwerk ontnomen. De devices kunnen op afstand gewhiped worden.

- De mobiele telefoons van medewerkers en inhuurkrachten worden gekoppeld aan een account ter verificatie. Daarnaast wordt Mobile Application Management toegepast waarmee een securityschil om de bedrijfsgegevens wordt aangebracht. Ook zijn de telefoons voorzien van antivirus software en verplichte vergrendeling met pin of facial recognition. De telefoons kunnen op afstand gewhiped worden.
- Voor beheeraccounts zijn strengere maatregelen getroffen zoals MFA bij elk gebruik, logging van handelingen en beperking van de ingelogde periode. Alle beheeraccounts zijn op naam en handelingen worden gelogd en zijn traceerbaar. Bij elk gebruik van een beheeraccount moet de reden worden opgegeven en moet koppeling met een serviceticket worden gelegd.
- Toegang tot informatie en het gebruik van functionaliteit gaat op basis van functieprofielen waarbij de principes 'Need to know' en 'Least privilege' zijn toegepast. De profielen worden beheerd in een matrix en periodiek wordt een IST-SOLL controle uitgevoerd door de eigenaar van de informatie of het systeem. Op betalingen en besluiten over kwijtschelding en declaraties wordt functiescheiding toegepast. Afhankelijk van het bedrag is dat door inzet van het vier- of zesogenprincipe.
- Voor veilige authenticatie bij applicaties wordt waar mogelijk gebruikt gemaakt van (secure) single sign on.
- Opslag van gegevens vindt alleen plaats in high-end datacenters waarin alle technische en procedurele industriestandaarden worden toegepast rondom bescherming van apparatuur en bekabeling, klimaatbeheersing, branddetectie- en blussystemen, noodstroomvoorziening, fysieke barrières en stringente procedures voor toegang, bediening en wijziging. Systemen worden gemonitord en er zijn procedures actief voor het behandelen van incidenten en afwijkingen.
- Https-verbindingen die door NHG worden beheerd zijn versleuteld met TLS1.2+ en scoren een A-niveau bij Qualys SSL Labs.
- E-mail wordt te allen tijde versleuteld verzonden en SPF, DKIM en DMARC zijn ingericht. Alle berichten en bijlagen die via e-mail worden ontvangen worden gescand op kwaadaardige signatures. Bij e-mails aan onze voornaamste ketenpartners wordt versleuteling hard afgedwongen.
- Voor de ICT-voorziening die wij aanbieden aan onze ketenpartners is een beleid voor veilig ontwikkelen geïmplementeerd waarin de best practices zoals peer review, secure libraries, inputvalidaties en de OWASP secure coding practices zijn opgenomen. Handelingen van beheerders en gebruikers worden gelogd en afwijkend gedrag zoals objectmanipulatie, injectie en de inzet van een securityscanner leidt tot een real-time alert.
- Bij de werving van nieuwe medewerkers is een Verklaring omtrent Gedrag verplicht, wordt minimaal 1 referentie gecontroleerd en wordt het relevante diploma geverifieerd. Nieuwe medewerkers en inhuurkrachten ondertekenen de gedragscode van NHG en worden gehouden de richtlijnen omtrent privacy en security na te leven.
- NHG stuurt actief op kennis en awareness door trainingen, workshops, simulaties en regelmatige berichtgeving over actuele dreigingen en hoe daarop te handelen.
- NHG heeft een vastgestelde procedure beveiligingsincidenten - waaronder datalekken - waarin is beschreven welke stappen moeten worden doorlopen om

adequate opvolging te geven aan het incident. Afdichten, schade beperken, oplossen, analyseren en evalueren zijn hierin de leidende onderwerpen.

Privacy

- De wettelijke grondslagen voor de verwerkingsactiviteiten van NHG zijn vastgelegd in het privacybeleid en in het privacybeleid wordt geduid hoe de beginselen uit de AVG moeten worden nageleefd.
- In het privacybeleid zijn relevante wettelijke bepalingen vertaald naar processen en praktische richtlijnen voor medewerkers.
- Klanten worden geïnformeerd over de verwerking van persoonsgegevens in de privacyverklaring van NHG op www.nhg.nl/privacy. Daarnaast wordt de klant op alle logische plekken waar persoonsgegevens worden gevraagd, gewezen op die informatie. Nieuwe klanten ontvangen een welkomstbrief waarin wordt verwezen naar de privacyverklaring. Ook in het bindend aanbod van de geldverstrekker wordt de klant gewezen op die verklaring.
- Sollicitanten en medewerkers worden geïnformeerd over de verwerkingsactiviteiten in de privacyverklaring werken en solliciteren bij NHG.
- In bovengenoemde privacyverklaringen, wordt de betrokkene geïnformeerd over diens rechten ten opzichte van NHG en de te volgen procedure voor het uitoefenen van die rechten zoals het recht op inzage, correctie, wissing, bezwaar of beperking. Bij NHG is een procedure actief waarin is beschreven hoe gehandeld moet worden als een betrokkene diens rechten uitoefent.
- NHG heeft een Beleid bewaartermijnen waarin is vastgelegd hoe lang gegevens worden bewaard en na welke termijn gegevens worden verwijderd.
- Bij nieuwe processen en producten of wijzigingen daarin wordt een privacy impact analyse uitgevoerd.
- Alle verwerkingsactiviteiten zijn vastgelegd in het register verwerkingsactiviteiten.
- NHG heeft een vastgestelde procedure meldplicht datalekken waarin is beschreven welke stappen moeten worden doorlopen om adequate opvolging te geven aan een datalek en om, indien van toepassing, tijdig aan de meldplicht te voldoen.
- Datalekken worden geadministreerd in een logboek waarin ook wordt vastgelegd wat de oorzaak van het incident is, welke maatregelen zijn getroffen ter afdichting en voorkoming, wat de aard van de persoonsgegevens is, de vermoedelijke gevolgen voor de verwerking en of sprake is van een melding aan de Autoriteit Persoonsgegevens en/of de betrokkene(n).
- NHG heeft een functionaris voor gegevensbescherming aangewezen die onafhankelijk toeziet op de naleving van de AVG en andere privacy wet- en regelgeving.
- Gegevens worden opgeslagen binnen de Europese Unie. Alleen indien het onvermijdelijk is, bijvoorbeeld om incidenten te verhelpen, kan het zijn dat gegevens worden ingezien van buiten de EU. Voor die gevallen zijn overeenkomsten afgesloten waarin waarborgen zijn getroffen om te voldoen aan de AVG.
- Er wordt actief gewerkt aan datakwaliteit door maatregelen als invoer-validaties, beperking van rechten, beperking van handmatige invoer, ICT Architectuur, controles bij externe bronnen, rapportages en correcties.

- Met alle derden die voor NHG persoonsgegevens verwerken is een verwerkers-overeenkomst afgesloten.
- Bij uitwisseling van persoonsgegevens met derden die ook Verwerkingsverantwoordelijke zijn, worden overeenkomsten afgesloten waarin passende waarborgen zijn opgenomen.
- Verdere verwerking voor andere doeleinden dan waarvoor de gegevens zijn verzameld wordt getoetst aan de vereisten van noodzaak, evenredigheid en verenigbaarheid.
- Er wordt documentatie aangehouden om de keuzes van NHG op het vlak van privacy te verantwoorden en uit te leggen.

Weerbaarheid
- Alle risico's die NHG heeft onderkend, worden minimaal jaarlijks en bij relevante wijzigingen aangevuld en/of herzien.
- Interne en externe ontwikkelingen worden gevolgd, mede aan de hand van trendrapportages van bijvoorbeeld NCSC, Gartner en ENISA.
- Elk kwartaal wordt de integrale risicorapportage besproken in het risico comité en de Auditcommissie; de Raad van Commissarissen (RvC) ontvangt daarvan een afschrift. Het risicobeheer is ingericht volgens het *three lines of defense* model.
- Als onderdeel van het kader voor ICT-risicobeheer heeft NHG bedrijfsnoodplannen die worden getest. Onderdeel daarvan is een procedure waarin is beschreven hoe communicatie over ernstige ICT-gerelateerde incidenten - indien van toepassing - aan ketenpartners, medewerkers, klanten en andere stakeholders plaats moet vinden.
- Verantwoordelijkheden en taken bij incidenten en calamiteiten zijn toegewezen, waaronder de verantwoordelijkheid van woordvoering aan publiek en media.
- NHG heeft geen legacysystemen en life cycle management en patching worden actief toegepast.
- Wijzigingen met een verhoogde risicofactor, zoals wijzigingen in netwerken, interfaces en authenticatievoorzieningen, worden door de security- en/of architectuurfunctie beoordeeld.
- NHG heeft een programma voor bewustmaking en training op het gebied van ICT-beveiliging en digitale operationele weerbaarheid voor het personeel, waaronder de Raad van Bestuur en Raad van Commissarissen.
- Processen zijn ingericht, en capaciteiten zijn aanwezig om informatie te verzamelen en ontwikkelingen te volgen over ICT-risico's en cyberdreigingen.
- Op de voornaamste ICT-systemen – waaronder de ICT-voorziening die wij aanbieden aan onze ketenpartners - wordt minimaal jaarlijks en bij relevante wijzigingen, bijvoorbeeld in de netwerk- en authenticatiemiddelen, een risicogebaseerde pentest uitgevoerd. Daarbij worden meerdere methoden toegepast, zoals white-box, black-box, configuratiecontroles, kwetsbaarhedenscans en code-review.
- De OWASP Top 10 meest voorkomende kwetsbaarheden worden in elke pentest geadresseerd.
- De pentesten worden uitgevoerd door externe partijen. Daarbij stellen wij de eis dat de testers een formele gedragscode hebben onderschreven.
- De bevindingen uit pentesten worden op basis van risico geprioriteerd en verholpen.

- NHG heeft een vastgesteld proces om ICT-gerelateerde incidenten te detecteren, beheren en melden. Alle ICT-gerelateerde incidenten en significante cyberdreigingen worden geregistreerd. Binnen het proces worden onderliggende oorzaken opgespoord, gedocumenteerd en geëvalueerd om herhaling van soortgelijke incidenten te voorkomen.
- Binnen het beheer van ICT-risico worden risico's op het vlak van leveranciers, zoals het risico op vendor lock-in beheerd. De uitbestedingsketen wordt daarnaast gemonitord en gecontroleerd aan de hand van assurance- en auditrapportages en service level rapportages.

Versie

Deze 'Weerbaarheid en security statement NHG' is versie 1.0. Deze versie is per 1 januari 2025 de opvolger van – en treedt per die datum ook in de plaats van – de 'Privacy & Security Statement'.