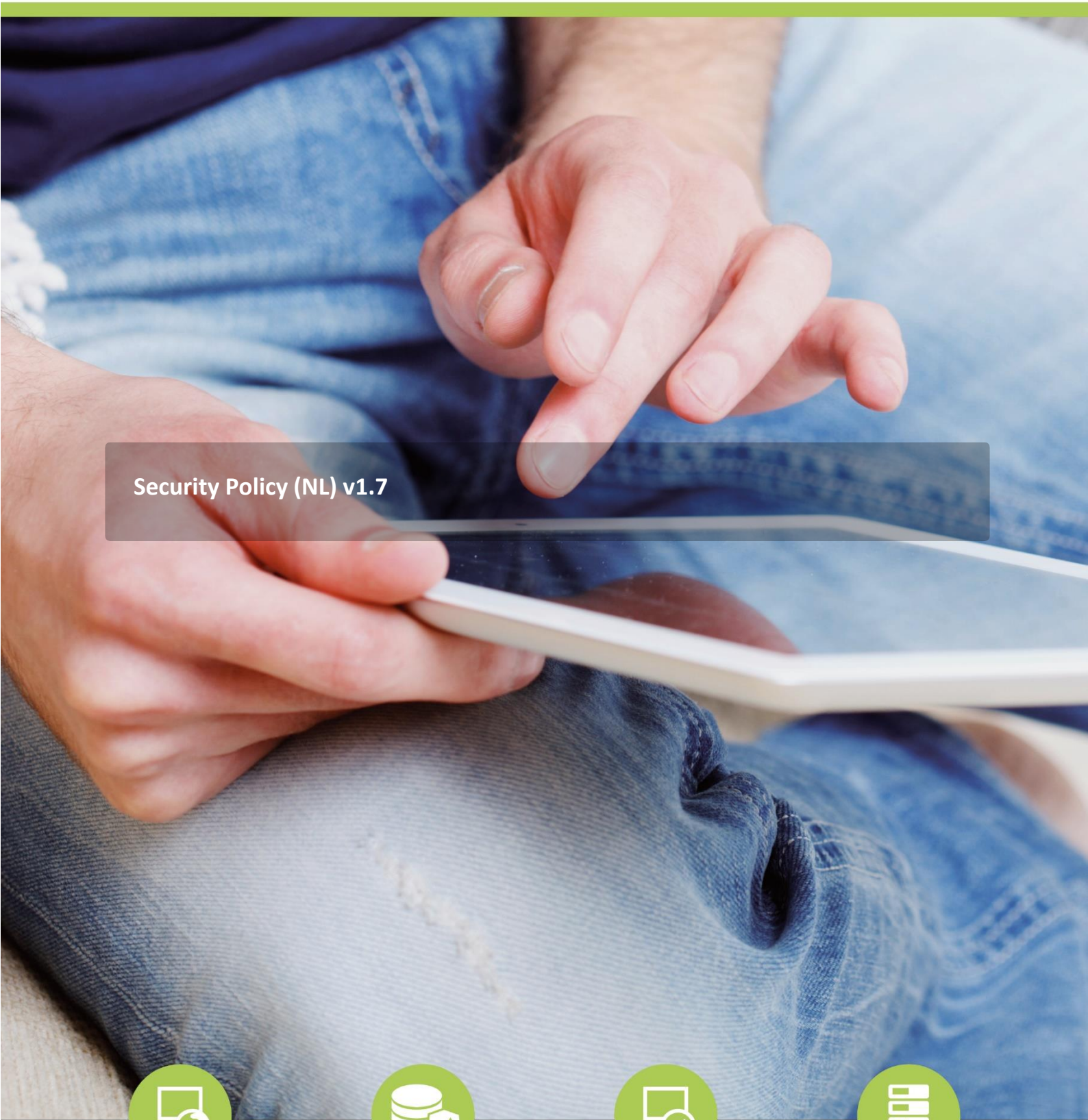
HARBERS ICT



Security Policy (NL) v1.7

Online werkplek

ICT uitwijk

Systeembeheer

Hostingdiensten

Author:	Erik Klein Langenhorst
Date:	6 juni 2018
Classificatie:	2 – Intended for stakeholders only

Versiehistorie

Versienr	Datum	Naam	Wijzigingen
0.1	*24-03-2016*	*Erik Klein Langenhorst*	*Initiële opzet*
1.0	*19-04-2016*	*Erik Klein Langenhorst*	*Aanvullingen aan maatregelen en risico's*
1.1	*19-04-2016*	*Erik Klein Langenhorst*	*Wijzigingen nav review Emiel Harbers*
1.2	*05-08-2016*	*Erik Klein Langenhorst*	*Wijzigingen nav bespreking*
1.3	*21-09-2017*	*Erik Klein Langenhorst*	*Aanvullingen terugvertaald vanuit Engelse versie*
1.4	*19-02-2018*	*Erik Klein Langenhorst*	*Onze interne maatregelen verduidelijkt en de standaardmaatregelen gemarkeerd met een **
1.5	*19-02-2018*	*Erik Klein Langenhorst*	*Geen wijzigingen – Versienummers gelijkgemaakt aan de Engelse versie*
1.6	*25-05-2018*	*Fedde Giesen*	*Subverwerkers van Harbers ICT toegevoegd aan het protocol*
1.7	*06-06-2018*	*Fedde Giesen*	*Wijzigingen aan hoofdstuk encryptiestandaard nav overleg*

Inhoud

Doel en achtergrond

Dit beveiligingsprotocol is deel van de overeenkomst die de klant (Verantwoordelijke) en Harbers ICT (verwerker) met elkaar hebben gesloten en vermeldt de technische en organisatorische maatregelen die Harbers ICT als bewerker kan implementeren. De meest recente versie van dit document is op ieder gewenst moment op te vragen bij Harbers ICT via support@harbersict.nl. Ook voor klanten die geen verwerkersovereenkomst met Harbers ICT hebben gesloten kan dit document als referentie gelden.

Onder de AVG (GDPR) is de Verantwoordelijke altijd degene die zich ervan moet vergewissen dat de maatregelen die beschreven worden afdoende zijn voor het type data dat wordt opgeslagen bij de Verwerker. Leest u dit document als Verantwoordelijke en heeft u vragen? Harbers ICT beantwoordt ze graag.

Dit document is vertaald vanuit het Engels ("Security Policy (EN) v1.7") en de Engelse versie is leidend.

Herzieningsfrequentie

Dit document wordt minimaal jaarlijks herzien. Het document kan ook herzien worden als belangrijke wijzigingen plaatsvinden in het beveiligingsbeleid van Harbers ICT. Harbers ICT mag het beveiligingsbeleid eenzijdig aanpassen, maar alleen zonder het niveau van de beveiliging te verminderen.

Aard van de verwerkingen

In het kader van de overeenkomst kan Harbers ICT verschillende verwerkingen uitvoeren, zoals Hosting van websites of webapplicaties, de cloudopslag van (persoons-)gegevens en de hosting van applicaties in online werkplekken. Harbers ICT stelt slechts de ICT infrastructuur ter beschikking waarbinnen de Verantwoordelijke de gegevens kan opslaan. De Verantwoordelijke bepaalt het doel en de middelen voor de verwerkingen.

Risico's

In het kader van de verwerking van de gegevens loopt de Verantwoordelijke risico op niet-geautoriseerde verwerking van data zoals beschadiging, ongeautoriseerde toegang en wijzigingen van de data. Als niet redelijkerwijs kan worden uitgesloten dat een inbreuk op de beveiligingsmaatregelen geleid heeft tot één van deze niet geautoriseerde acties, dient dit volgens EU wetgeving beschouwd te worden als datalek. De risico's worden hieronder beschreven.

Ongeautoriseerde toegang

Iemand verschaft zich, bijvoorbeeld door middel van het omzeilen van beveiligingsmaatregelen of procedures ongeautoriseerde toegang tot de gegevens.

Onbedoelde vernietiging of aantasting

De gegevens van de Verantwoordelijke raken vernietigd of aangetast. De oorzaak zou bijvoorbeeld een virus of malware kunnen zijn maar het kan ook veroorzaakt worden door een menselijke fout.

Het niet beschikbaar zijn van de omgeving

In het geval van het niet beschikbaar zijn van de omgeving is de data nog aanwezig maar kunt u deze als Verantwoordelijke niet benaderen als gevolg van (infrastructurele) problemen aan de kant van Harbers ICT.

Maatregelen

Harbers ICT zal zich inspannen om een adequaat niveau van beveiliging te garanderen tegen misbruik en ongeautoriseerd gebruik van de door haar verwerkte gegevens zoals beschreven in de verwerkersovereenkomst. Harbers ICT kan de volgende maatregelen treffen om de risico's tegen te gaan. De daadwerkelijk te nemen maatregelen zijn beschreven in de overeenkomst of SLA.

De standaardmaatregelen zijn gemarkeerd met een *. Deze maatregelen worden altijd genomen, onafhankelijk van de dienst die u afneemt.

Encryptie (versleuteling) van digitale bestanden met persoonsgegevens*

Als er voor de verwerking van uw data de noodzaak bestaat dat uw digitale bestanden getransporteerd worden - zowel fysiek als digitaal - dan zullen wij ervoor zorgen dat de bestanden en/of verbinding versleuteld zijn. Wij gebruik hiervoor minimaal de onderstaande encryptiestandaarden.

Encryptiestandaarden:

- Key exchange (Phase1 VPN): Diffie–Hellman key exchange with minimum 2048 bits
- Message Integrity: HMAC-SHA2
- Message Hash: SHA2 256 bits
- Assymetric encryption: RSA 2048 bits
- Symmetric-key algorithm (Phase2 VPN): AES 128 (voorkeur) en 3DES (indien gewenst door klant).
- Password Hashing: PBKDF2, Scrypt, Bcrypt, SHA2.

Logische toegangscontrole, namelijk door middel van een wachtwoord en een Token*

Harbers ICT online werkplekken beschikken over toegangscontrole door middel van een wachtwoord en een 2-factor authenticatietoken. Een 2-factor authenticatietoken is een persoonlijk identificatienummer dat u kunt genereren middels een app op uw telefoon of een apparaatje. Andere diensten zijn alleen met een wachtwoord beveiligd. Dit geldt bijvoorbeeld voor Webmail.

Andere optionele technische maatregelen voor netwerkbeveiliging

Afhankelijk van de diensten die u afneemt nemen wij de volgende technische maatregelen om uw diensten te beveiligen.

- ⇨ Netwerkpartitionering en Isolatie:
  - Ons netwerkdesign omvat een VLAN configuratie om onze servers in segmenten te verdelen. Iedere klant ontvangt in principe een eigen VLAN, tenzij anders gespecificeerd.
- ⇨ Threat Prevention, bestaande uit:
  - Next Generation Firewall*
  - Application Control
    - De Application Control Software Blade controleert de toegang naar meer dan 5200 applicaties en 240.000 social network widgets. Dit is de grootste applicatiedekking in de industrie. Het is hiermee mogelijk om een fijnmazig beveiligingsbeleid te creëren om webapplicaties en widgets zoals instant messaging, social networking, videostreaming etc. te herkennen en blokkeren of limiteren.
  - Anti-Bot
    - De Anti-Bot Software Blade detecteert computers die geïnfecteerd zijn met een bot en voorkomt schade door de communicatie van de bot met het Command en Control center te blokkeren en wordt continu geüpdatet vanuit ThreatCloud
  - Antivirus
    - De Antivirus Software blade stopt inkomende kwaadwillende bestanden nog voordat deze de gebruiker bereikt. Real-time virusdefinities en bescherming tegen onregelmatigheden kunnen meer dan 4,5 miljoen malwarehandtekeningen en meer dan 300.000 schadelijke websites herkennen met een constant geüpdatet wereldwijd netwerk van sensoren die inlichtingen verschaffen over huidige malwareaanvallen.
  - Identity Awareness
    - Met de Identity Awareness softwareblade bieden we nauwkeurig inzicht in gebruikers, groepen en machines, waardoor we ongeëvenaarde applicatie en toegangscontrole kunnen bieden met behulp van op identiteit gebaseerd beleid.
  - Anti-Spam en Email security
    - Met de Anti-Spam en Email Security Software blade bieden we uitgebreide bescherming voor ons berichtenplatform. Een multidimensionele aanpak beschermt onze emailinfrastructuur, biedt zeer nauwkeurige ant-spamdekking en beschermt u tegen een grote verscheidenheid aan virus en malwarebedreigingen.

- Intrusion Prevention System*
  - IPS biedt een compleet Intrusion Prevention System beveiligingsoplossing, die uitgebreide netwerkbescherming biedt tegen kwaadwillend en ongewenst netwerkverkeer, waaronder:
    - Malwareaanvallen
    - Dos en DDoS aanvallen
    - Applicatie- en serverkwetsbaarheden
    - Bedreigingen van binnenuit
- URL Filtering
  - De URL Filtering softwareblade controleert de toegang tot miljoenen websites op basis van categorie, gebruikers, groepen en machines met cloudgebaseerde technology die constant wordt geüpdatet met nieuwe websites om de productiviteit en beveiliging van uw medewerkers te garanderen.

Antivirussoftware*

We installeren moderne antivirussoftware op onze eigen servers en op de servers/VPS'en van onze klanten.

Spamfiltering*

Voor ons mailplatform gebruiken we een Barracuda Email Security Gateway. Dit is een emailbeveiligingsgateway die alle inkomende en uitgaande emailverkeer filtert en beheert om uw organisatie te beschermen tegen bedreigingen en datalekken die voortkomen uit uw emailverkeer.

Backups*

We gebruiken gespecialiseerde backupsoftware om uw data te backuppen. Wij hebben een eigen backupinfrastructuur in een het datacenter van Equinix in Zwolle. Tussen deze datacenters ligt een rechtstreekse verbinding waarop alleen wij toegang hebben. Retentietijden variëren per product en worden gespecificeerd in uw SLA of Service Agreement. We bieden fijnmazige restore opties waarmee we losse bestanden, e-mail items, AD items of een gehele VPS kunnen herstellen.

VPN*

We gebruiken een netwerksetup met meerdere beschermingslagen en een afgescheiden beheernetwerk. We gebruiken Check Point Endpoint Remote Access VPN software om op een veilige manier te verbinden met ons beheernetwerk. Als we voor onszelf of onze klanten site-to-site (VPN) tunnels opzetten dan gebruiken wij veilige encryptiestandaarden zoals gedefinieerd onder "*Encryptiestandaarden*".

DDoS bescherming

Distributed Denial of Serviceaanvallen komen steeds meer voor en kunnen uitval van netwerken binnen onbeschermde infrastructuren veroorzaken. We bieden Equinix AntiDDoS defense als een optionele service tegen DDoS aanvallen. Zie voor meer informatie: http://www.equinix.nl/services/managed-services/security-performance/anti-ddos/

Beveiligde verbindingen*

Alle verbindingen naar onze sites, portals en supportsysteem zijn met TLS beveiligd. We bieden ook de mogelijkheid de websites die we hosten voor onze klanten met TLS te beveiligen (tegen een meerprijs). Waar dit mogelijk is gebruiken we alleen sterke Ciphersuites en protocollen.

Server Hardening

Waar toepasbaar volgen we richtlijnen die opgezet zijn door het Center for Internet Security voor server hardening for Microsoft Windows Server. Zie voor meer informatie: https://www.cisecurity.org/cis-benchmarks/.

Beveiligd intern netwerk*

Organisatorische en fysieke maatregelen zijn ook van toepassing op ons interne netwerk. Het is voor medewerkers niet mogelijk zonder toestemming toegang tot de interne serverruimte te krijgen.

Endpointbeveiliging*

Uiteraard is ook ons eigen kantoornetwerk beveiligd middels een Next-generation firewall. Al onze computers zijn voorzien van een virusscanner en onze mail wordt gefilterd door de Barracuda spamfiltering die we ook inzetten voor onze klanten. We gebruiken BitLocker encryptie voor onze Windows computers en op onze macOS computers gebruiken we FileVault encryptie.

Organisatorische maatregelen voor toegangsbeveiliging en Doelgebonden toegangsbeperkingen*

Alleen medewerkers die toegang nodig hebben voor de uitvoering van hun werkzaamheden, hebben inzage in de persoonsgegevens. Zij hebben een geheimhoudingsverklaring met een boeteclausule getekend. Daarnaast bieden wij de mogelijkheid u te voorzien van een NDA (Non-Disclosure Agreement) waarin wij contractueel met u vastleggen dat wij de toegang voor niets anders zullen gebruiken dan voor noodzakelijke verwerkingen.

Wij voorzien onze medewerkers op regelmatige basis van training om hen er op te wijzen wat het belang is van het beschermen van klant- en medewerkerdata en hen te wijzen op hun rol hierin.

We hebben procedures ingericht om toegangsrechten van medewerkers aan te passen of in te trekken bij een wijziging of beëindiging van het dienstverband.

Fysieke maatregelen voor toegangsbeveiliging*

De hostingdiensten die Harbers ICT levert worden vanuit een beveiligd datacentrum van Equinix aangeboden. Toegang tot de apparatuur is slechts mogelijk voor een beperkt aantal medewerkers en alleen na het tonen van identificatie. Toegang voor externe leveranciers wordt alleen toegestaan onder supervisie van een van onze medewerkers. De ruimte staat onder permanente (video-)bewaking.

Steekproefsgewijze controle op naleving beleid

Regelmatig wordt gecontroleerd of de toegangsbeperkingen correct zijn en of de overige punten uit het beleid van Harbers ICT correct worden nageleefd. Harbers ICT werkt bovendien aan de implementatie van een beveiligingsbeleid op basis van ISO 27001. Deel van de implementatie is een regelmatige audit door een externe partij.

Subverwerkers van Harbers ICT

In onderstaand tabel zijn de Subverwerkers van Harbers ICT opgenomen. Op basis van de dienst(en) die u afneemt bij ons kan het zijn dat wij één of meerdere van deze Subverwerkers inschakelen om de dienst(en) aan u te leveren.

Naam Subverwerker	**Dienst**	**Product**	**Doel van doorgifte**
Check Point Software Technologies	Security	Check Point Firewall	Activatie Check Point Firewall
Cisco Meraki	Managed Wifi	Meraki	Aanbieden dienst en support
Cisco Systems, Inc.	Managed Wifi	Cisco	Aanbieden dienst en support
Citrix Systems, Inc.	Online werkplekken	Citrix	Aanbieden dienst en support
Dell Inc.	Hardware levering	-	Als leverancier gegevens nodig heeft voor uitleveren van de order
DigiCert Inc.	Security	SSL certificaat	Uitvoeren van de dienst
ESET	Antivirus	ESET Endpoint Security	Aanvragen licentie / aanbieden dienst en support
Ingram Micro	Hard-/software levering	-	Als leverancier gegevens nodig heeft voor uitleveren van de order
Mail Chimp	-	-	Uitvoeren van de dienst
Microsoft Corporation	Office 365	Office 365	Aanbieden dienst en support
Tech Data	Hard-/software levering	ESET Endpoint Security	Als leverancier gegevens nodig heeft voor uitleveren van de order
TransIP	Domeinregistratie	-	Uitvoeren van de dienst
Trend Micro	Antivirus	Trend Micro Antivirus	Aanvragen licentie / aanbieden dienst en support
Ubiquiti Networks	Managed Wifi	Ubiquiti UniFi	Aanbieden dienst en support
Veeam Software	Back-up	Veeam back-up	Aanvragen licentie / aanbieden dienst en support
Westcon-Comstor NL	Hard-/software levering	Check Point Firewall	Als leverancier gegevens nodig heeft voor uitleveren van de order
Xink	E-mail handtekening	Xink	Uitvoeren van de dienst
Xolphin	Security	SSL certificaat	Uitvoeren van de dienst

Tabel 1 - Subverwerkers Harbers ICT

Uitsluitingen

Dit document is alleen van toepassing op cloud- en hostingdiensten die Harbers ICT aanbiedt. Voor beheerdiensten op klantlocaties speelt Harbers ICT alleen een adviserende rol. Klanten blijven zelf verantwoordelijk voor de beveiliging van hun netwerk en data.

Voor sommige van onze producten zijn de leveringsvoorwaarden van een derde partij van toepassing. Dit geldt bijvoorbeeld voor Office 365, waarbij de voorwaarden van Microsoft van toepassing zijn. In het algemeen geldt dit voor producten geleverd door derde partijen waarbij Harbers ICT geen invloed heeft op de mate van beveiliging.