Informatiebeveiliging

Version: Versie 1.1, vastgesteld op 27 januari 2015

Status: Statement voor cliënten

Informatiebeveiliging van voor Holla van cruciaal belang. Wij zijn ons bewust van het bedrijfskritische karakter van de beschikbaarheid en vertrouwelijkheid van de cliënt- en dossiergegevens. Daarom voorziet Holla in een solide integrale informatiebeveiliging, waarmee Holla zich ten opzichte van andere kantoren differentieert.

---

1. Doel van dit document

Een ijzersterke beveiliging van de cliënt- en bedrijfsinformatie van Holla is cruciaal. Dit document is bedoeld om bestaande relaties van Holla te informeren over de maatregelen en voorzieningen die Holla treft het oog op waarborging van een goede informatiebeveiliging. Het document geeft een algemene beschrijving, zonder daarbij gedetailleerd en volledig te beogen te zijn.

2. Wie we zijn en wat we doen

Holla Poelman van Leeuwen Advocaten N.V. (“Holla”) is een full service advocatenkantoor dat juridische diensten levert aan de (groot)zakelijke markt. Meer informatie over Holla vindt men hier.

3. Informatiebeveiligingsbeleid

Holla heeft een integraal informatiebeveiligingsbeleid dat zich richt op constante aandacht voor en verbetering van de diverse aspecten van informatiebeveiliging, waaronder op de procedurele, fysieke en organisatorische aspecten (o.a. instroom en uitstroom van personeel, inzet externen/leveranciers, wachtwoordcomplexiteit, idle-time, juiste classificatie hantering van data, technische redundanties, etc. en keuze voor en inzet en configuratie van onderdelen in de diverse OSI-lagen).

4. ICT-omgeving

De organisatie heeft de afgelopen jaren flikt geïnvesteerd in een moderne ICT omgeving, inclusief de nodige IT-security voorzieningen waaronder een realtime antivirusscanners, exchange mailscanner, firewalls en gateways met DPI (Deep Packet Inspection).

Holla maakt gebruik van een zgn. *thin client* architectuur, waardoor alle zakelijke data enkel toegankelijk is via een beveiligde Citrix omgeving. Alle zakelijke data bevindt zich uitsluitend in een beveiligd datacentrum in (uitsluitend) Nederland.

Op werkplekniveau zijn thin clients zodanig ingericht dat er lokaal geen zakelijke data beschikbaar is en dat er lokaal uitsluitend een Citrix verbinding tot het datacentrum kan worden opgezet. Iedere andere mogelijkheid om een (ongeautoriseerde) internetverbinding tot stand te brengen of om zakelijke data via USB of optische media (o.a. cd-rom) te exporteren is in beginsel kantoor-breed geblokkeerd. Om het risico van dataverlies of -diefstal verder te minimaliseren worden aan de advocaten, secretaresses en overige medewerkers van Holla geen zakelijke data lokaal beschikbaar gesteld op smartphones, tablets of laptops.

5. Business Continuity

Om het risico van dataverlies te minimaliseren wordt iedere 30 minuten een snapshot van de productiedata (fileserver) gemaakt. Daarnaast vindt iedere 24 uur een incrementele back-up plaats van alle productiedata (waaronder de fileserver, exchangeomgeving, het document management systeem, etc.).

Met het oog op business continuity wordt bovendien iedere maand een integrale back-up gemaakt van de gehele ICT-omgeving, inclusief alle configuratiedata.

Om redenen van redundantie wordt alle back-up data versleuteld weggeschreven op een eigen beveiligde, derde locatie (eigen NAS-inrichting van Holla). In aanvulling daarop wordt een kopie van de back-up data ook versleuteld opgeslagen op een vierde locatie van de leverancier.

Bij de inrichting van onze ICT-architectuur is met het oog op business continuity bewust gekozen voor een thin cliënt architectuur, waarmee de afhankelijkheid van een fysieke werkomgeving sterk wordt verminderd.

6. Holla domein en email

Alle websites van Holla zijn voorzien van SSL certificaten met SHA256 TLS1.2 beveiliging. Inloggen op ons kantoornetwerk kan alleen m.b.v. een RSA SecurID token.

Alle e-mail communicatie van Mailserver naar Outlook/TelSync/Webmail wordt enkel toegestaan via HTTPS ofwel een SSL-certificaat. (met SHA256 encryptie). Uitgaande e-mail wordt bovendien standaard voorzien van een SSL Mail-certificaat. (die eveneens voorzien zijn van een SHA256 encryptie).

7. Online datatransfer

Voor de aanlevering door en overdracht van grotere hoeveelheden data aan cliënten en relaties dan (secure mail) kan verwerken, hanteert Holla een oplossing genaamd Cryptshare, dat voorzien is van een SHA1 encryptie SSL certificaat. Gebruik van applicaties als Wetransfer etc. is technisch uitgesloten / beperkt.

8. Gescheiden netwerken

Om de ICT-kwetsbaarheid te minimaliseren hanteert Holla gescheiden wifi netwerken: een apart gastennetwerk, dat volledig is gescheiden van het bedrijfs(wifi)netwerk.

9. Periodieke security audits

Tenslotte brengt ons informatiebeveiligingsbeleid met zich mee dat Holla periodiek een integrale security audit laten uitvoeren door een POB1104 gekwalificeerd digitaal recherchebureau. Een en ander omvat een integrale controle op onze informatiebeveiliging, waaronder op de werkprocessen, procedures en fysieke werkomgeving. Ook zgn. penetration testing (d.w.z. ethical hacking op onze netwerken, systemen, applicaties en websites) maakt onderdeel uit van deze periodieke security audits.

In aanvulling op voornoemde voorzieningen heeft Holla uiteraard nog een reeks aan aanvullende maatregelen getroffen, waarover Holla – met het oog op een effectieve borging van de informatiebeveiliging – echter niet extern communiceert.

10. Contact

Als u naar aanleiding van de informatie in dit document nog vragen heeft of nadere toelichting wenst, kunt u contact met ons opnemen via:

- email: privacy@holla.nl; or
- telefonisch: +31 88 44 02 400

* * *