HULPDOCUMENT GEDRAGSCODE INFORMATIEBEVEILIGING

Van Brug Software

Versie 1.1

Inhoud

Inleiding

Dit is een ondersteunend document van Van Brug Software.

Van Brug Software heeft als kerntaken het leveren, ontwikkelen en beheren van notariële en juridische software (Codex en Online Dossier) en bijbehorende ondersteuning bieden voor dienstverleners.

Dit document kan als openbare informatie worden behandeld. Het bevat geen gevoelige informatie, zoals adressen van personen en autoriteiten en gegevens betreffende de bedrijfsvoering.

De CISO van Van Brug Software of de organisatie zelf is niet verantwoordelijk voor de uitvoering en implementatie van de beheersmaatregelen op de gedragscode.

Doelstelling

Dit hulpdocument is bedoeld om te gebruiken bij de implementatie van de beheersmaatregelen uit de Gedragscode Informatiebeveiliging Notariaat. Het doel is om hulp te bieden bij de onderwerpen en hoofstukken die raakvlakken hebben met de softwareleverancier. Van Brug Software host namelijk delen van de software online. Hierdoor zijn wij ook SaaS-leverancier en leveren daarmee ICT-diensten. Door een expliciete uitleg wordt duidelijk waar de scheidslijn ligt tussen notariskantoor, systeembeheerder en softwareleverancier.

Het hulpdocument besteedt dus geen aandacht aan de maatregelen die los staan van de softwareleverancier, Van Brug Software.

Doelgroep

De doelgroep die baat heeft bij dit document heeft zijn klanten die gebruik maken van diensten en producten van Van Brug Software. Codex, Online Dossier, Van Brug Robot, Van Brug invoegtoepassingen voor Microsoft 365 en toekomstige SaaS-modules vallen hieronder. Voor het gemak zijn alle relevante hoofstukken die raakvlakken hebben met ons als softwareleverancier geel gemarkeerd. Daarnaast hebben wij andere hoofdstukken voorzien van tips & tricks.

Toelichtingen per hoofdstuk

1 Beleid en organisatie

1.1 Beleid

Geen raakvlakken met Van Brug Software

1.2 Organisatie

Geen raakvlakken met Van Brug Software

1.3 Contact ten aanzien van informatiebeveiliging

Contact ten aanzien van informatiebeveiliging kan met Van brug Software. Voor kennisdeling, incidenten of datalekken zijn onze contactgegevens:

E-mail: support@vanbrug.nl
Telefoonnummer: 085 - 2020307

2 Uitwisseling gegevens

2.1 Uitwisseling gegevens

Vaak worden gegevens nog steeds uitgewisseld per e-mail. Echter wordt dit niet aangeraden omdat er nog wel eens wat fout gaat. Dit kan het beste via een beveiligde separate omgeving. Een portal waar beide partijen bestanden en gegevens kunnen uploaden en downloaden. E-mail beveiligen is natuurlijk wel belangrijk, daarover later meer.

In de gedragscode wordt vanuit punt ‘b’ verwezen naar: “Onder ‘beveiligd informatie aanleveren’ verstaan we dat dit gebeurt op een wijze dat de informatie niet zonder meer door onbevoegden kan worden ingezien, bijvoorbeeld door het gebruik van een veilige uitwisselomgeving.”

Uiteraard zijn er tal van portals beschikbaar maar Van Brug Software biedt de mogelijkheid om vanuit Codex het Online Dossier direct te gebruiken. Vanuit Codex wordt een beveiligde verbinding gelegd om bestanden uit het cliëntdossier te uploaden naar Online Dossier en te downloaden naar het dossier in Codex. Ook de notificatie naar de cliënt dat er het één en ander klaarstaat kan vanuit Codex worden verstuurd. Is de cliënt klaar, dan ontvangt U vanuit Codex een bericht.

Zoals aangegeven is het beveiligen van e-mail wél noodzakelijk. Er wordt namelijk behoorlijk wat informatie uitgewisseld via e-mail, ook persoonsgegevens. Bespreek met uw systeembeheerder daarom de mogelijkheden. SPF, DKIM en DMARC zijn belangrijke technische instellingen die uw e-mail veel veiliger maken en moeilijker te ‘spoofen’.

- SPF, oftewel Sender Policy Framework is een protocol dat tot doel heeft spam te verminderen. Hierbij wordt vastgesteld dat degene die de e-mail verstuurd ook echt de eigenaar is van het e-mailadres waarvan verstuurd wordt.
- DKIM, oftewel DomainKeys Identified Mail, is een authenticatiemethode waarmee e-mailberichten kunnen worden gewaarmerkt. Aan de hand van dit waarmerk kan de ontvanger afleiden of de e-mail daadwerkelijk van het domein van de verzender komt én of de inhoud van het bericht na het versturen door derden is gemanipuleerd.
- DMARC, oftewel Domain-based Message Authentication, Reporting, and Conformance is een verificatieprotocol voor e-mail. Het is ontworpen om de beheerders van e-maildomeinen de mogelijkheid te geven hun domein te beschermen tegen ongeoorloofd gebruik, beter

bekend als e-mail spoofing. U kunt hiermee uw ontvangstservers laten weten wat ze moeten doen met uitgaande berichten van uw organisatie die niet door de SPF- of DKIM-controle komen.

3 Gegevens en documenten

3.1 Registratie en classificatie van informatie

Geen raakvlakken met Van Brug Software maar wel een tip. Een classificatieschema is eenvoudig op te stellen, zie onderstaand voorbeeld. In het voorbeeld daarna zijn voorbeelden van beschermingsmaatregelen beschreven:

	Classificatie		
Aspect	**Openbaar**	**Intern**	**Vertrouwelijk**
Soort informatie	Overige informatie	Informatie om de bedrijfsmatige samenwerking tussen medewerkers van het notariskantoor te ondersteunen.	Informatie voor beperkte verspreiding naar personeel, zakelijke partners of relaties met derden, 1 op 1 communicatie met collega's.
Mogelijke gevolgen openbaar worden	Bij openbaar worden heeft informatie geen noemenswaardige impact op het notariskantoor	Als deze informatie buiten het notariskantoor terecht komt, kan dit een nadelig effect hebben op de organisatie, haar zakelijke partners en/of relaties met derden	Als deze informatie ongewenst openbaar wordt, heeft dit een negatieve invloed op het notariskantoor, haar zakelijke partners of relaties met derden
Voorbeelden	- Productbeschrijvingen - Productspecificaties - Flyers - Inhoud van de website	- Personeelshandboek - Procesbeschrijvingen - ICT Infrastructuur - Incidentrapport	- Personeelsdossier - Salarisadministratie - MT-verslagen - Gegevens klanten

Voorbeeld classificatieschema

	Maatregelen		
Bedrijfsmiddel	**Openbaar**	**Intern**	**Vertrouwelijk**
Papier	Geen	- Labelen (Intern) - Niet achterlaten op werkplek - Vernietigen met papiervernietiger	- Labelen (Vertrouwelijk) - Afgesloten bewaren - Aangetekend versturen - Vernietigen met papiervernietiger
Permanente opslag	Geen	- Opslaan op een SharePoint schijf of toegewezen systeem	- Opslaan op een toegewezen systeem
Verwijderebare opslag (USB-sticks, mobiele harddisks)	Gebruik van verwijderbare opslag is **niet** toegestaan.	- Gebruik van verwijderbare opslag is **niet** toegestaan.	- Gebruik van verwijderbare opslag is **niet** toegestaan.
Mobiel device (Notebook, tablet, smartphone)	Geen	- Encryptie toepassen - Device voorzien van een veilige pincode en/of wachtwoord - Ter vernietiging aanbieden bij gecertificeerd bedrijf	- Toestemming nodig van informatie-eigenaar - Encryptie toepassen - Vastleggen ontvangst - Device voorzien van een veilige pincode en/of wachtwoord - Ter vernietiging aanbieden bij gecertificeerd bedrijf
E-mail	Geen	- Encryptie toepassen naar oordeel van informatie-eigenaar	- Toestemming nodig van informatie-eigenaar - Vastleggen ontvangst - Encryptie toepassen

Voorbeeld beschermingsmaatregelen bij classificatieschema.

4 Toegang tot informatie en systemen

4.1 Toegang tot informatie en systemen

De systeembeheerder draagt zorg voor de gewenste autorisaties in het systeem. Dit doet hij in overleg met de notaris. Wanneer je Codex kan starten kun je in dossiers.

Codex biedt een Personeel Management Systeem (PMS) die zorgt voor eenduidige toegang met verschillende rechten. Zorg dat algemene accounts worden verdeeld over échte gebruikers (dus geen 'receptie' o.i.d.).

Tip: Het is belangrijk bij het afhandelen van de punten dat er een autorisatiematrix wordt opgesteld. Hiermee wordt in één keer duidelijk wie waarin toegang heeft. Dit kun je voor meerdere systemen inrichten zoals SharePoint of een Windows mappen systeem:

	Administratie map	Financieel	Iedereen@notariskantoor.nl	Groep X
Gebruiker 1			X	X
Gebruiker 2	X	X	X	
Gebruiker 3	X		X	

Voorbeeld autorisatiematrix

Vaak heeft de systeembeheerder al een matrix opgesteld. Dit geldt ook voor het instellen van een wachtwoordbeleid. Neem hiervoor met hen contact op tenzij u dit zelf beheerd.

Bij Punt 'o' wordt gesproken over vertrouwde netwerkzondes die een verwijzing maakt naar hoofdstuk 8. Hierin hebben wij wel een aantal belangrijke opmerkingen.

Geplande aanpassingen vanaf 2024 op autorisaties binnen Codex

Eind 2023 wordt de AD-integratie toegevoegd aan Codex. Een AD integratie betekent dat iemand toegang heeft tot Codex als:

- Een gebruiker een account in het AD heeft
- Eén van de volgende Codex rollen in het AD heeft: Notaris, Behandelaar of Beheerder. Andere rollen kunnen nog worden toegevoegd. Geen rol betekent geen toegang in Codex. Dit geldt op latere termijn ook voor de Microsoft Office add-ins.
- Het account actief is.

In de eerste helft van 2024 willen we uitgebreide autorisaties gaan toevoegen aan Codex. In de praktijk betekent dit dat:

- De gebruiker moet voldoen aan de eerdergenoemde punten.
- Specifieke vensters en acties per rol geautoriseerd kunnen worden:
    - Beheeromgeving en programma's zoals de applicatiemanager voor beheerders.
    - Acties alleen voorbehouden aan de Notaris (zoals ondertekenen).
    - Privacygevoelige schermen met informatie over cliënten en medewerkers.
- Alle niet beschermde vensters en knoppen beschikbaar zijn voor alle gebruikers.

Autorisatie op Dossier niveau (wat mag een gebruiker zien?):

- Een Notaris en een Behandelaar hebben altijd toegang tot het dossier.
- Medewerkers kunnen los toegevoegd worden aan een dossier.

- Wanneer een vestiging aan het dossier wordt toegevoegd, worden deze medewerkers standaard toegevoegd. Door het vinkje “medewerkers autoriseren” uit te zetten, krijgen geen van de vestigingsmedewerkers toegang.
- Op het autorisatie venster van het dossier kan met een druk op de knop alle medewerkers van een vestiging toegevoegd worden.
- Ook kan dit per medewerker geautoriseerd worden.

- Als een notariskantoor valt onder een gezamenlijk label, kunnen medewerkers van de vestigingen gegevens van de cliënten van beide locaties zien.
- Op het overzichtsvenster van dossiers zal privacy toegepast worden. Sommige kolommen zullen hierdoor niet zichtbaar zijn.

Additionele aanpassingen:

- De toegang tot een dossier wordt gelogd, inclusief wijzigingen.
- Bij de SharePoint integratie worden autorisaties op mappen ingesteld. De autorisatie op dossiers (wie mag erbij?) wordt ook op de dossiermap toegepast. Eventueel doen we dit op Fileshare niveau.

5 Fysieke maatregelen

5.1 Kantoorpanden

Geen raakvlakken met Van Brug Software. Wel wat tips. Kantoorpanden zijn vaak al voorzien van verschillende zones maar zijn dan niet beschreven. Een afgesloten ruimte, bijvoorbeeld een archief is zo’n zone. Met een plattegrond met daarin de zones beschreven kun je vaak alle bevraging dekkend krijgen. Neem mee in de autorisatiematrix wie er precies toegang hebben tot welke zone.

Met clear-screen-principe wordt bedoeld dat er geen documenten rondslingeren op het bureaublad van de digitale werkplek. Plaats documenten in mappen en sla deze op de juiste locatie op.

5.2 Apparatuur (inclusief gegevensdragers)

Geen raakvlakken met Van Brug Software. Wel een tip.

Sta geen mobiele gegevensdragers toe zoals USB-sticks of andere draagbare opslag.

6 Beveiligingsincidenten

6.1 Herkennen en afhandelen van beveiligingsincidenten

Geen raakvlakken met Van Brug Software.

Tip: Maak één document met daarin de beveiligingsincidenten, risico’s, actiepunten en datalekken.

6.2 Melden van ernstige beveiligingsincidenten aan KNB

Geen raakvlakken met Van Brug Software.

7 Medewerkers en bewustzijn

7.1 In dienst

Geen raakvlakken met Van Brug Software.

7.2 Tijdens dienstverband

Geen raakvlakken met Van Brug Software.

7.3 Uit dienst

Geen raakvlakken met Van Brug Software.

Tip: Het is handig om voor deze werkzaamheden een checklist te maken.

8 IT-security management

8.1 Inventarisatie bedrijfsmiddelen

Geen raakvlakken met Van Brug Software.

Tip: Maak een makkelijke en overzichtelijke lijst van notebooks, smartphones, software en (cloud)diensten). Vermeld bij de hardware minimaal het merk, type en serienummer.

8.2 IT-documentatie

Geen raakvlakken met Van Brug Software.

Tip: Met instructie wordt letterlijk een bedieningsprocedure bedoeld. Omschrijf de bediening van een systeem en wie dit moet kunnen.

8.3 Back-up en restore

Wij maken dagelijks back-ups van onze SaaS-diensten. Deze back-ups worden één jaar bewaard op een beveiligde locatie. Elk kwartaal wordt de werking getest van het back-up systeem en de data.

Codex staat bij u lokaal of op een server in een datacenter geïnstalleerd. Dit geldt dus ook voor de dossiers, archief en database. De back-ups over deze data moet worden uitgevoerd door uw systeembeheerder.

8.4 Bescherming tegen malware

Geen raakvlakken met Van Brug Software.

Tip: Maakt u gebruik van Microsoft 365, schaf dan ook een ATP (Advanced Threat Protection) licentie aan. Dit scheelt veel werk en er wordt constant gemonitord of er dreiging of risico's zijn.

8.5 Beheer van wijzigingen van applicaties en systemen

Codex maakt inmiddels gebruik van de auto-updater. Zo garanderen wij dat u altijd op de laatste versie werkt met de nieuwste mogelijkheden. Uw systeembeheerder kan dit voor u instellen. Onze SaaS-applicaties draaien altijd op de laatste versie.

8.6 Patching en updates

Codex maakt inmiddels gebruik van de auto-updater. Zo garanderen wij dat u altijd op de laatste versie werkt met de laatste beveiligingsupdates. Uw systeembeheerder kunt dit voor u instellen. Onze SaaS-applicaties draaien altijd op de laatste versie. Bij ernstige kwetsbaarheden zal er dírect actie ondernomen worden.

Tip: Staan er Windows updates klaar op uw systeem, pas deze direct toe. Zo loopt u het minste risico.

8.7 Encryptie

Geen raakvlakken met Van Brug Software.

Tip: Beveiligingssleutels kun je ook automatisch opslaan. Overleg met uw systeembeheerder.

8.8 Netwerken

Geen raakvlakken met Van Brug Software.

8.9 Monitoring en logging

Al onze SaaS-diensten worden gemonitord en gelogd. De logging staat 365 dagen op een separate server opgeslagen bij onze Azure specialist.

8.10 Aanschaf en ontwikkeling van informatiesystemen

Dit onderdeel is van toepassing op Van Brug Software en vind je terug in onze overeenkomsten.

I. Op ál onze software vindt actieve ondersteuning plaats op basis van ontwikkeling en support.
II. Onze software voldoet aan paragraaf 8.3 voor back-up en restore.
III. Onze software ondersteunt de eisen uit paragraaf 4.1 door middel van het Personeel Management Systeem (PMS).
IV. Het behandelen van bestanden gebeurt via Codex maar is op de achtergrond een Windows handeling en daarom zullen uw bestanden door de anti-malware programma's worden gescand. SaaS-diensten bij Van Brug Software worden online gescand.
V. Wij passen de DevSepOps methode toe en ons ISO27001 certificaat vereist ook dat wij wettelijke en contractuele eisen naleven.

Wij maken daarnaast nog gebruik van een gescheiden productie-, ontwikkel- en testomgeving. Ook maken wij voor onze acceptatieomgeving actief gebruik van werkgroepen die onze software testen. Deze onderdelen worden bij onze pilotkantoren genoemd. Daarnaast hebben wij een adviesraad, bestaande uit een groep klanten welke ons adviseren over de wijzigingen die het beste doorgevoerd kunnen worden.

9 Continuïteits- en calamiteitenmanagement

9.1 Opstellen continuïteits- en calamiteitenplan

Geen raakvlakken maar Van Brug Software heeft een Bedrijf Continuïteit Plan (BCP).

9.2 Testen continuïteits- en calamiteitenplan

Geen raakvlakken maar Van Brug Software test het BCP jaarlijks met telkens een ander scenario. Hier worden alle SaaS-platformen in meegenomen.

Betrek altijd de systeembeheerder bij deze activiteiten. Bij het herstel van het systeem is er bij hen een sterke afhankelijkheid.

10 Dienstenleveranciers

10.1 Eisen aan dienstenleveranciers

Wij voldoen aan de gestelde leveranciersafspraken uit de gedragscode. Vanuit onze overeenkomsten zoals het SLA en de verwerkersovereenkomst worden de verantwoordelijkheden van onze kant belegd.

10.2 Afspraken met dienstenleveranciers

Wij voldoen aan de gestelde leveranciersafspraken uit de gedragscode.

10.3 Beoordeling van dienstenleveranciers

Het is aan u om te bepalen of wij voldoende aan de door u gestelde eisen voldoen. Neem met ons contact op om de leveranciersafspraken nog eens te controleren:

Bijlage A: Checklist gedragscode informatieveiligheid

Het doel van deze pagina is dat u overzicht houdt welk onderdeel u al afgewerkt heeft.

Hoofdstuk	Titel	Checkbox
1	**Beleid en organisatie**	☐
1.1	Beleid	☐
1.2	Organisatie	☐
1.3	Contact ten aanzien van informatiebeveiliging	
2	**Uitwisseling gegevens**	☐
2.1	Uitwisseling gegevens	
3	**Gegevens en documenten**	☐
3.1	Registratie en classificatie van informatie	
4	**Toegang tot informatie en systemen**	☐
4.1	Toegang tot informatie en systemen	
5	**Fysieke maatregelen**	☐
5.1	Kantoorpanden	☐
5.2	Apparatuur (inclusief gegevensdragers)	
6	**Beveiligingsincidenten**	☐
6.1	Herkennen en afhandelen van beveiligingsincidenten	☐
6.2	Melden van ernstige beveiligingsincidenten aan KNB	
7	**Medewerkers en bewustzijn**	☐
7.1	In dienst	☐
7.2	Tijdens dienstverband	☐
7.3	Uit dienst	
8	**IT-security management**	☐
8.1	Inventarisatie bedrijfsmiddelen	☐
8.2	IT-documentatie	☐
8.3	Back-up en restore	☐
8.4	Bescherming tegen malware	☐
8.5	Beheer van wijzigingen van applicaties en systemen	☐
8.6	Patching en updates	☐
8.7	Encryptie	☐
8.8	Netwerken	☐
8.9	Monitoring en logging	☐
8.10	Aanschaf en ontwikkeling van informatiesystemen	
9	**Continuïteits- en calamiteitenmanagement**	☐
9.1	Opstellen continuïteits- en calamiteitenplan	☐
9.2	Testen continuïteits- en calamiteitenplan	
10	**Dienstenleveranciers**	☐
10.1	Eisen aan dienstenleveranciers	☐
10.2	Afspraken met dienstenleveranciers	☐
10.3	Beoordeling van dienstenleveranciers	