Securitybeleid Dstny Nederland
Technische en organisatorische beleidsregels

Dstny Nederland
Versie 1.0 NL
1-8-2021

Als Dstny Nederland streven wij ernaar om constante kwaliteit te leveren op elk vlak van onze dienstverlening en bouwen wij iedere dag verder aan de allerbeste dienstverlening en service op het gebied van cloud telefonie. Het voldoen aan wettelijke en reglementaire informatiebeveiligingsvereisten is hier een belangrijk onderdeel van.

Dstny Nederland voldoet hieraan en dit vertaalt zich naar het Informatiebeveiligingsbeleid conform ISO27001. Het Informatiebeveiligingsbeleid van Dstny Nederland is van toepassing op alle bedrijfsfuncties binnen het toepassingsgebied van het Informatiebeveiligingsbeheersysteem en omvat de informatie, informatiesystemen, netwerken, fysieke omgeving en mensen die deze bedrijfsfuncties ondersteunen. In dit document staan de Informatiebeveiligingsdoelstellingen en het beleid van Dstny Nederland centraal.

Doelstellingen

Het doel van Informatiebeveiliging is het waarborgen van de bedrijfscontinuïteit en het minimaliseren van bedrijfsschade door het voorkomen en minimaliseren van de impact van beveiligingsincidenten. Met name moeten informatiemiddelen worden beschermd om te zorgen voor:

1. Vertrouwelijkheid, d.w.z. bescherming tegen ongeoorloofde openbaarmaking.
2. Integriteit, d.w.z. bescherming tegen ongeoorloofde of accidentele wijziging.
3. Beschikbaarheid waar en wanneer nodig voor het realiseren van de bedrijfsdoelstellingen.

Organisatie, rollen en verantwoordelijkheden

1. De directie heeft dit Informatiebeveiligingsbeleid goedgekeurd en is hiervoor eindverantwoordelijk.
2. De Security officer is verantwoordelijk voor het beheer van dit Informatiebeveiligingsbeleid en voor het onderhoud van de daarmee samenhangende documenten binnen dit managementsysteem.
3. De Security officer is daarnaast verantwoordelijk voor de bevordering van het bewustzijn en de naleving van het beleid door de organisatie.
4. Dstny Nederland heeft een Information Security Team dat verantwoordelijk is voor de uitvoering van het Informatiebeveiligingsbeleid.
5. De dagelijkse verantwoordelijkheid voor procedurele aangelegenheden, het onderzoek van incidenten, de rapportage over het beheer, enz. berust bij de Security officer.
6. De dagelijkse verantwoordelijkheid voor en de contacten met externe organisaties voor de naleving van de wettelijke eisen, met inbegrip van de bescherming van gegevens, berusten bij de Data Protection Officer (DPO).
7. Alle werknemers of dienstverleners namens de organisatie hebben de plicht om de middelen, inclusief locaties, hardware, software, systemen of informatie, die zij onder hun hoede hebben, te beschermen en elke vermoede inbreuk op de beveiliging onmiddellijk te melden.
8. Bij alle dagelijkse activiteiten, processen, plannen, projecten, contracten en samenwerkingsverbanden van de organisatie wordt rekening gehouden met informatiebeveiligingsaspecten.

9. Het naleven van informatiebeveiligingsprocedures zoals uiteengezet in de beleids- en procedurestukken wordt geaccepteerd als onderdeel van de standaardwerkwijzen binnen de organisatie.
10. Gezien de positie van Dstny Nederland als professional in het leveren van cloud telefonie met behulp van informatiesystemen, bronnen en middelen, wordt er bij alle procedures en door alle medewerkers bijzondere zorg besteed aan het waarborgen van de informatiebeveiliging en gegevensoverdracht van zijn klanten.
11. Dstny Nederland voldoet aan alle wettelijke en reglementaire vereisten en er wordt regelmatig op wijzigingen gecontroleerd.
12. Dstny Nederland beschikt over een bedrijfscontinuïteitsplan. Dit plan wordt door het Information Security Team onderhouden, getest en regelmatig herzien.
13. Dit Informatiebeveiligingsbeleid wordt regelmatig herzien en kan door de Security officer worden gewijzigd om de blijvende levensvatbaarheid, toepasbaarheid en naleving van de wetgeving te waarborgen en om de informatiebeveiligingssystemen voortdurend te verbeteren.

Mobiele Computers en telewerken

In de Dstny Nederland 'Securitybeleid' zijn o.a. beveiligingsmaatregelen vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt, te beheren.

Naast maatregelen m.b.t. mobiele apparatuur van eigen Dstny Nederland medewerkers, zoals alle soorten draagbare computers, mobieltjes, tablets, geheugenkaarten en andere draagbare apparaten gebruikt voor opslag, verwerking en overdragen van gegevens, gaat eveneens de nodige aandacht uit naar:

- Privé mobiele apparatuur.
- Laptop of pc van derden in Dstny Nederland – gebouw.

Informatie is uitsluitend bereikbaar vanaf door Dstny Nederland beheerde omgevingen.

Ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen, zijn ook de nodige ondersteunende beveiligingsmaatregelen geïmplementeerd, zoals bijvoorbeeld het voorzien van alle noodzakelijke infrastructuur om veilig en snel een verbinding met Dstny Nederland te kunnen opzetten.

Medewerkers en contractanten (voor, tijdens en na dienstverband)

Dstny Nederland waarborgt dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen. Vooraleer iemand in dienstverband te nemen, zal Dstny Nederland in overeenstemming met haar 'strategisch plan HR' de nodige screening via twee of meerdere specifieke interviewtechnieken alsook een (beperkte) technische test (ivt) uitvoeren, in overeenstemming met relevante wet- en regelgeving en ethische overwegingen.

In het arbeidsreglement is opgenomen dat de werknemers zich dienen te houden aan de richtlijnen die Dstny Nederland heeft opgesteld omtrent informatiebeveiliging in haar 'Securitybeleid'. In deze ook bijzondere aandacht voor de geheimhouding van Dstny Nederland en klantgegevens. De Dstny Nederland medewerkers en, voor zover relevant, contractanten krijgen een passende bewustzijnsopleiding en -training en regelmatige bijscholing van de Dstny Nederland - beleidsregels en procedures, voor zover relevant voor hun functie. Dstny Nederland heeft een gedetailleerd sanctiebeleid uitgeschreven in de arbeidsovereenkomst, om, ingeval van mogelijke inbreuk op informatiebeveiliging,

conform een formele en gecommuniceerde disciplinaire procedure de nodige acties te kunnen ondernemen. Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband zijn ook gedefinieerd en gecommuniceerd aan de medewerker of contractant.

Classificatie van informatie

Dstny Nederland bewerkstelligt dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan, door informatie te classificeren conform de wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging. Op deze manier worden door de toegekende verantwoordelijke(n) de nodige beveiligingsmaatregelen geactiveerd voor bepaalde type van Data, zodat de risico's worden geminimaliseerd.

Verantwoordelijkheden voor bedrijfsmiddelen

Dstny Nederland heeft procedures voor het behandelen van bedrijfsmiddelen geïmplementeerd in overeenstemming met bovenvermeld informatieclassificatieschema. Bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten worden geïdentificeerd, en van deze bedrijfsmiddelen, die specifiek worden toegekend aan een eigenaar, houdt Dstny Nederland een inventaris (Asset Management) bij. Er zijn regels opgesteld en gecommuniceerd, voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten. Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die zij in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst teruggeven.

Behandeling van media

Dstny Nederland wil ten alle tijden onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie, die op media is opgeslagen, voorkomen. Daartoe volgt Dstny Nederland procedures m.b.t. :

- Het beheer van verwijderbare media, conform bovenvermeld classificatieschema.
- Het verwijderen van media, op een veilige en beveiligde manier, als ze niet langer nodig zijn.
- Het transport van media, die informatie bevatten.

Cryptografische beheersmaatregelen

Ter bescherming van informatie maakt Dstny Nederland correct en doeltreffend gebruik van cryptografie, om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

Toegangscontrole & beveiligde gebieden

Dstny Nederland voorziet de nodige toegangsbeveiliging om ervoor te zorgen dat toegang tot voorzieningen en gegevens enkel mogelijk is voor gebruikers die daartoe zijn gerechtigd. De nodige procedures en controles zijn geïmplementeerd, opdat gebruikers alleen toegang krijgen tot het netwerk, de netwerkdiensten, applicaties, waarvoor zij specifiek bevoegd zijn. Hierbij denken we o.a.:

- Strikte inlogprocedures.
- Zich houden aan vooropgestelde regels bij het gebruiken van geheime authenticatieinformatie, geregeld via interactieve systemen voor wachtwoordbeheer.

Ook op fysiek niveau heeft Dstny Nederland de beveiligingszones gedefinieerd die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten, en zodoende de nodige bescherming krijgen. Via specifieke fysieke toegangsbeveiligingsprocedures wordt gewaarborgd dat enkel bevoegd personeel toegang krijgt. Ook wordt op regelmatige basis specialistisch advies ingewonnen over het voorkomen van schade door brand, overstroming, aardbeving, explosie, burgerlijke onrust en andere vormen van natuurrampen of door de mens veroorzaakte rampen.

Beveiliging van apparatuur

Verlies, schade, diefstal of onderbreking van de bedrijfsvoering van de organisatie wordt door Dstny Nederland voorkomen door:

- Apparatuur zo te plaatsen en te beschermen dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.
- Apparatuur te beschermen tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.

Hier maken we een onderscheid tussen:

Infrastructuur in Datacenters

In onze datacenters zijn volgende voorzieningen getroffen om apparatuur te beschermen tegen verstoringen in nutsvoorzieningen:

- Energie.
- Klimaatbeheersing.
- Vochtdetectiesysteem.
- Brandveiligheid.
- Bliksembeveiliging.
- Aarding.
- Communicatie.

Infrastructuur in eigen gebouwen

Om onze infrastructuur in eigen gebouwen te beschermen tegen mogelijke stroomuitval:

- Zijn de servers gekoppeld op UPS'sen.
- Worden de servers continue gemonitord, zodat een uitval door een stroomonderbreking onmiddellijk opgemerkt wordt.

Dstny Nederland zorgt voor het correct onderhouden van apparatuur om de continue beschikbaarheid en integriteit ervan te waarborgen. Tevens legt Dstny Nederland op dat apparatuur, informatie en software, behorend tot classificatie geheim, zonder uitdrukkelijke toestemming van het management niet buiten het kantoorgebouw mogen worden meegenomen (digitaal of op papier), of op systemen buiten het kantoorgebouw mogen worden geplaatst (door verzenden, opslaan, uploaden, etc.). Afwijking hierop kan gebeuren via specifieke aanvraag bij de directe manager.

Clean desk – clear screen

Clean desk

Dstny Nederland legt aan haar werknemers op dat, indien men niet op zijn werkplek zit, zowel alle papieren, alsook gegevensopslagmedia gelabeld als gevoelig (classificatie: geheim of vertrouwelijk), van het bureau of andere plaatsen (printers, kopieerapparaten, enz.) moeten worden verwijderd om ongeautoriseerde toegang te voorkomen. Dergelijke documenten en media dienen op een veilige manier te worden opgeslagen in overeenstemming met het Dstny Nederland 'beleid voor geclassificeerde Informatie'.

Clear screen

Ook dient, indien men niet op zijn werkplek zit, alle gevoelige informatie van het scherm te worden verwijderd, en dient de toegang tot alle schermen én tot alle systemen waarvoor de persoon autorisatie heeft te worden geweigerd.

Printers, copiers en fysieke postdocumenten die gevoelige informatie (geheim of vertrouwelijk) bevat worden direct van de printers, fax en kopieerapparaten verwijderd. Verzamelplekken voor ontvangen of nog te verzenden fysieke post, worden door afsluiting beveiligd. Vertrouwelijke post wordt alleen geopend door de geadresseerde persoon of afdeling.

Bedieningsprocedures en verantwoordelijkheden

Dstny Nederland waarborgt een correcte en veilige bediening van informatieverwerkende faciliteiten, door het voorzien van:

- Gedocumenteerde bedieningsprocedures.
- Procedures om veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging te beheersen.
- Gebruik van named accounts bij inlogprocedures.
- Gebruik van MFA bij inlogprocedures.
- Adequate capaciteitsbeheer.
- Scheiding van ontwikkel-, test- en productieomgevingen.

Bescherming Malware

Ter bescherming tegen Malware heeft Dstny Nederland de nodige beheersmaatregelen geïmplementeerd voor detectie, preventie en herstel, in combinatie met een passend bewustzijn van gebruikers.

Back-up

Om te beschermen tegen het verlies van gegevens maakt Dstny Nederland regelmatig de nodige back-upkopieën van informatie, software en systeemafbeeldingen en test deze conform het intern back-upbeleid.

Logging en bewaking

Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, worden gemaakt, bewaard en regelmatig door of in opdracht van het Dstny Nederland Management beoordeeld. Deze logfaciliteiten en informatie in logbestanden worden beschermd tegen vervalsing en onbevoegde toegang

Beheer van netwerkbeveiliging

Dstny Nederland waarborgt een degelijke bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten. Dit dankzij een adequaat beheer om netwerken te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd. Met het oog hierop worden groepen van informatiediensten, -gebruikers en -systemen in netwerken gescheiden.

Informatie-uitwisseling

Dstny Nederland handhaaft de beveiliging van informatie dat wordt uitgewisseld binnen de organisatie en met een externe entiteit. Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, zijn binnen Dstny Nederland formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht. Ook voor informatie dat is opgenomen in elektronische berichten wordt in een passende bescherming voorzien.

Rapportage van informatiebeveiligingsgebeurtenissen

Dstny Nederland bewerkstelligt een consistente en doeltreffende aanpak van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.

- Informatiebeveiligingsgebeurtenissen alsook vermeende zwakke plekken in de informatiebeveiliging worden zo snel mogelijk via de juiste leidinggevende niveaus gerapporteerd.
- Informatiebeveiligingsgebeurtenissen worden beoordeeld en er wordt geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.
- Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen wordt gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen. Daartoe zal er na ieder beveiligingsincident een ‘lessons learned’ actiepunt worden opgezet.

Sint-Oedenrode, 1 augustus 2021

Ed Smit
Managing Director Dstny Nederland