Beleid voor Informatiebeveiliging en Milieubeleid

Inhoudsopgave

Milieubeleid

Introductie

Voor iSOC24 B.V. (hierna iSOC24) gaat Verantwoord Ondernemen verder dan alleen voldoen aan wet- en regelgeving. Binnen het manifest zijn drie ambities voor de langere termijn geformuleerd:

1. We zijn een mensgerichte organisatie: wij streven naar hoge waarderingscijfers bij zowel klanten als medewerkers.
2. We zijn een maatschappelijke organisatie: we willen waarde creëren voor onze klanten met eenvoudige, verantwoorde producten en diensten.
3. We zijn een duurzame organisatie: we werken toe naar een klimaat neutrale organisatie, waarbij we onze eigen bedrijfsvoering verduurzamen en klanten actief stimuleren om energie te besparen.

Verantwoord Ondernemen betekent ook dat we stilstaan bij alle gevolgen van ons handelen. Natuur en milieu moeten ontzien worden en mensenrechten mogen nooit worden geschonden. Daar houden we rekening mee als we investeringen doen en bij onze interne bedrijfsvoering. Diezelfde houding verwachten we ook van onze leveranciers. Samen willen we werken aan een duurzaam inkoopproces door duurzaam te denken en duurzaam te doen.

Implementatie milieumanagementsysteem (ISO 14001)

iSOC24 ziet de noodzaak om zich aantoonbaar meer bezig te houden met de belasting van haar activiteiten op het milieu. Hiervoor hebben we een milieumanagementsysteem opgezet en geïmplementeerd conform de ISO 14001 eisen, om zo milieubelastende activiteiten verder te beheersen en waar mogelijk te reduceren. Hiervoor zijn reeds mogelijkheden geïdentificeerd t.a.v. afvalscheiding, reductie papierverbruik, verlaging brandstofverbruik, het gebruik van meer milieuvriendelijkere / duurzame producten, het verduurzamen van de huisvesting en het motiveren van samenwerkingspartijen en leveranciers om meer rekening te houden met het milieu.

- iSOC24 heeft een milieumanagementsysteem (ISO 14001 milieucertificatie).
- iSOC24 heeft een milieuprogramma, waarvan onderdelen zijn:
    - Terugdringing van de CO_2-uitstoot van de bedrijfsvoering.
    - Terugdringing van het gebruik en/of vervanging van materiaal en materiaal dat schadelijk is voor de omgeving.
    - Terugdringing van het watergebruik.
    - Terugdringen van elektriciteit.
    - Vermindering en recycling van haar afval.
- iSOC24 heeft een beleid voor duurzame inkoop.
- iSOC24 rapporteert over de voortgang en laat dit extern controleren.
- iSOC24 reduceert waar mogelijk met haar maatregelen de impact op het milieu.
- iSOC24 houdt rekening met maatschappelijke belangen.

Informatiebeveiliging

Introductie

Informatiebeveiliging staat bij iSOC24 hoog in het vaandel. Het beveiligen van uw data is een van onze hoogste prioriteiten. We zijn voorstander van transparantie over onze beveiligingsprincipes en helpen u graag om onze benadering te begrijpen.

Onze beveiliging is afgestemd op de ISO 27001 norm en wordt regelmatig gecontroleerd en beoordeeld door derde partijen.

Beveiliging van personeel

Personele maatregelen zijn van toepassing op alle tijdelijke en vaste, interne en externe medewerkers en leveranciers die toegang hebben tot iSOC24, haar interne informatiesystemen en/of toegang tot iSOC24's kantoorruimte. Alvorens toegang wordt afgegeven voor systemen moeten alle medewerkers akkoord gaan met de geheimhoudingsverklaring, een achtergrond screening doorstaan en een securitytraining bijwonen. Deze training omvat privacy- en security onderwerpen, inclusief device security, acceptabel gebruik, voorkomen van malware, fysieke beveiliging, dataprivacy, accountbeheer, wachtwoordbeheer, en incidentrapportage. Bij beëindiging van de werkzaamheden wordt alle toegang tot systemen onmiddellijk uitgeschakeld.

Security en privacy training

Tijdens het dienstverband moeten alle medewerkers minstens een keer per jaar hun kennis van privacy en security opfrissen. De medewerkers ondertekenen dat zij de informatiebeveiligingsbeleidstukken hebben gelezen en zich daaraan houden. Sommige medewerkers, zoals beheerders en ondersteunend personeel, die extra toegang tot systemen of gegevens hebben, krijgen aanvullende werk specifieke training over privacy en beveiliging. Medewerkers zijn verplicht om veiligheids- en privacy problemen te melden. Medewerkers zijn geïnformeerd dat niet-naleving van beleid gevolgen tot zelfs beëindiging van het dienstverband kunnen opleveren.

Toegewezen security professionals

iSOC24 heeft rollen en verantwoordelijkheden gedefinieerd om te bepalen welke rollen in de organisatie verantwoordelijk zijn voor de werking van de verschillende aspecten van haar Managementsysteem voor Informatiebeveiliging (ISMS). De verantwoordelijkheden van elke rol zijn gedetailleerd beschreven in onze beveiligingsdocumenten.

iSOC24 heeft een ISMS Manager aangesteld met de algemene verantwoordelijkheid voor de implementatie en het beheer van haar ISMS.

Beleid en standaarden

iSOC24 onderhoudt een reeks beleidsdocumenten, normen, procedures en richtlijnen die de medewerkers de weg wijzen voor het gebruik van ons ISMS. Onze beveiligingsdocumenten zorgen ervoor dat onze klanten erop kunnen vertrouwen dat onze medewerkers zich veilig en ethisch gedragen. De beleidsdocumenten zijn levende documenten: ze worden regelmatig beoordeeld en bijgewerkt en indien nodig beschikbaar gesteld aan de medewerkers op wie zij van toepassing zijn.

Audits, wet- en regelgeving, en derde partij beoordelingen

Audits

iSOC24 evalueert het design en de operatie van haar ISMS voor de naleving van interne en externe normen. iSOC24 laat zich beoordelen door externe auditors. Auditresultaten worden gedeeld met het management en alle bevindingen worden opgevolgd.

Wettelijke naleving
iSOC24 maakt gebruik van toegewijde juridische en compliance professionals. Deze professionals zijn ingebed in de ontwikkelingscyclus en beoordelen producten en eigenschappen of ze voldoen aan de wettelijke vereisten.

Bescherming van klantengegevens

De focus van iSOC24's securityprogramma is om ongeautoriseerde toegang tot klantengegevens te voorkomen. Daartoe neemt ons team uitgebreide stappen om risico's te identificeren en te beperken, om de best practices te implementeren en voortdurend te evalueren om te verbeteren.

Meer informatie over privacy vindt u in ons Privacybeleid op https://www.isoc24.com/docs/isoc24-privacy-statement-nl-25-mei-2018-v1.1.pdf.

Netwerkbeveiliging

Binnen iSOC24 zijn regels opgesteld voor het versturen van informatie over publieke netwerken. De methode en het niveau van beveiliging wordt bepaald aan de hand van de toegewezen classificatie van de informatie.

Classificatie en opslaan van data

Binnen iSOC24 wordt informatie geclassificeerd aan de hand van de volgende criteria:

- Waarde van de informatie gebaseerd op de gevolgen beoordeeld gedurende risicobeoordeling.
- Gevoeligheid en kritiekheid van informatie gebaseerd op het hoogst berekende risico voor elk item van informatie gedurende risicobeoordeling.
- Wetgeving en contractuele verplichtingen gebaseerd op de Lijst Wet-, Regelgeving en Contractuele Verplichtingen.

Er wordt onderscheid gemaakt tussen classificatie niveaus waarbij elk classificatie niveau is gekoppeld aan een set beveiligingsmaatregelen.

Geautoriseerde toegang

Om de risico's van gegevensblootstelling te minimaliseren, volgt iSOC24 het principe van *need to know*. Medewerkers hebben alleen toegang tot gegevens die ze redelijkerwijs nodig hebben om hun huidige taken te vervullen. Om dit te handhaven gebruikt iSOC24 de volgende maatregelen:

- De toegang van elke gebruiker wordt regelmatig beoordeeld om ervoor te zorgen dat de toegekende toegang nog steeds geschikt is voor de huidige werkverantwoordelijkheden van de gebruiker.
- Om het risico van onbevoegde toegang tot data verder te verminderen, past iSOC24 waar mogelijk twee-factor-authenticatie toe voor toegang tot systemen van derden.
- iSOC24 vereist dat personeel een goedgekeurde wachtwoordmanager gebruikt. Wachtwoordmanagers genereren, opslaan en invoeren unieke en complexe wachtwoorden. Gebruik van een wachtwoordmanager helpt bij het voorkomen van wachtwoordhergebruik, phishing en ander gedrag dat de beveiliging kan reduceren.

Systeem monitoring, logging en alarmering

Binnen iSOC24 zijn rollen en verantwoordelijkheden vastgesteld voor zowel het controleren van de logs van automatisch gerapporteerde fouten als ook voor het registreren van fouten gerapporteerd door gebruikers om te analyseren waarom fouten optreden en om geschikte corrigerende acties te nemen.

Bring Your Own Device (BYOD)

iSOC24 ondersteunt het gebruik van BYOD voor zakelijk gebruik. Dit geldt alleen voor medewerkers die anders niet in staat zouden zijn om het werk op een andere wijze uit te voeren. Er wordt een lijst bijgehouden van de functienamen en/of welke medewerkers die BYOD mogen gebruiken, tezamen met de applicaties en databases waartoe zij toegang mogen hebben met hun eigen apparaten.

Daarnaast stelt iSOC24 diverse regels aan het gebruik van BYOD en is er een minimumconfiguratie vereist voor elk type device.

Reageren op incidenten

Elke medewerker, leverancier of een andere derde partij die in contact komt met informatie en/of systemen van iSOC24 dient elke bedreiging, incident of gebeurtenis aan een systeem die zou kunnen leiden tot een mogelijk incident aan de ISMS Manager te melden. Er zijn diverse procedures ontwikkeld om snel en adequaat te reageren op incidenten. Alle incidenten worden regelmatig beoordeeld en geëvalueerd om ervan te leren.

Verwijdering en vernietiging van apparatuur en media

Binnen iSOC24 worden regels gehanteerd over het verwijderen en/of vernietigen van apparatuur en media voordat het wordt weggegooid, verkocht, gedoneerd, verzonden, gerepareerd, hergebruikt of aan een andere gebruiker wordt gegeven.

Clear desk & clear screen

Binnen iSOC24 wordt er gewerkt conform het clear desk en clear screen beleid. Dit houdt in dat indien de geautoriseerde persoon niet op zijn/haar werkplek zit, dient hij/zij de informatie, papieren, opslagmedia, van het bureau of andere plaatsen zoals printers, kopieerapparaten etc. moeten worden verwijderd om ongeautoriseerde toegang te voorkomen. Op dezelfde wijze geldt dat alle gevoelige informatie van het beeldscherm verwijderd dient te worden en dat schermvergrendeling wordt toegepast wanneer de geautoriseerde persoon zijn/haar werkplek verlaat.

Bedrijfscontinuïteit

iSOC24 heeft diverse plannen en procedures opgesteld, die er voor zorgen dat haar bedrijfscontinuïteit blijft gewaarborgd.

Derde partijen

Om de business efficiënt te runnen vertrouwt iSOC24 op dienstverlenende organisaties. Waar de dienstverlenende organisaties de secundaire productie van iSOC24 kunnen beïnvloeden, neemt iSOC24 maatregelen om ervoor te zorgen dat het beveiligingsniveau wordt gewaarborgd. iSOC24 legt afspraken vast die vereisen dat dienstverleners zich houden aan de verplichtingen die iSOC24 aan hen heeft gesteld. Indien noodzakelijk, iSOC24 controleert ten minste een keer per jaar de effectieve werking van de beveiligingsmaatregelen van de organisatie.

Conclusie

Bij iSOC24 staat informatiebeveiliging hoog in het vaandel omdat iedereen die onze dienst gebruikt van ons mag verwachten dat deze gegevens veilig en vertrouwelijk zijn. Beveiliging van deze gegevens is een kritische verantwoordelijkheid die we aan onze klanten hebben en we werken er hard aan om dat vertrouwen te behouden.