Over Laurens & Nivard IT Services

Laurens & Nivard IT Services is een club van resultaatgerichte, enthousiaste en professionele IT'ers met meer dan vijfentwintig jaar expertise. We begrijpen wat het betekent als het netwerk onbereikbaar is, printers niet printen en devices niet werken. Daarom zetten we ons met onze expertise 24/7 in om 'downtime' te voorkomen en dreigingen van buitenaf te pareren. We zitten niet tegenover, maar naast u, want partnerschap is waarnaar we streven. Dat begint met vertrouwen.

Toepassingsgebied

Om de kwaliteit van de output van de organisatie te optimaliseren, worden de processen en bedrijfsvoering van Laurens & Nivard IT Services goed geborgd en blijven we deze optimaliseren. Daarnaast vinden we het belangrijk dat onze informatiebeveiliging op een zo hoog mogelijk niveau is en ook deze blijven we optimaliseren.

Om dit te bewerkstelligen heeft Laurens & Nivard IT Services een managementsysteem opgezet en geïmplementeerd conform de eisen van de norm ISO-9001:2015 en de ISO-27001:2022.

De scope conform het kwaliteitsmanagementsysteem ISO 9001 is bepaald als:
Het ontwerpen, implementeren, beheren en ondersteunen van IT-omgevingen, waaronder managed werkplekken, cloud- en infrastructuuroplossingen, netwerkbeheer, monitoring, support en de levering van netwerkverbindingen.

De scope conform het informatiebeveiligingsmanagementsysteem ISO 27001 is bepaald als:
Het waarborgen van informatiebeveiliging met betrekking tot het ontwerpen, implementeren, beheren en ondersteunen van IT-omgevingen, waaronder managed werkplekken, cloud- en infrastructuuroplossingen, netwerkbeheer, monitoring, support en de levering van netwerkverbindingen.

Kwaliteitsbeleid

Het kwaliteitsbeleid van Laurens & Nivard IT Services bevat algemene doelstellingen van Laurens & Nivard IT Services t.a.v. kwaliteit. Het voldoen aan de verwachtingen van klanten en relevante belanghebbenden en het continu verbeteren van de interne organisatie staat daarin centraal. Dit wordt gedaan door:

1. Een voor de organisatie passend beleid te ontwikkelen;
2. Dit beleid kenbaar te maken binnen de organisatie;
3. Het bevorderen van kwaliteitsbewustzijn bij medewerkers;
4. Het motiveren van medewerkers, waarbij betrokkenheid bij verbeterprojecten wordt gestimuleerd;
5. Het faciliteren van trainingen en/of opleidingen van medewerkers
6. Regelmatig overleg te hebben met klanten over de eisen die aan de te leveren producten en diensten gesteld dienen te worden;
7. Continu te streven naar verhoging van de klanttevredenheid;
8. Te voldoen aan geldende wet- en regelgeving;
9. Een kwaliteitsmanagementsysteem te onderhouden dat voldoet aan de voorwaarden zoals gesteld in de norm ISO-9001:2015

Een combinatie van risico-inventarisaties, interne projectevaluaties, klanttevredenheidsanalyses en interne audits draagt bij aan het identificeren van mogelijke verbeteringen binnen de processen van onze organisatie. Door het analyseren van informatie en het implementeren van verbeteringen op basis van deze informatie ontstaat een lerende organisatie waar continue verbetering op basis van de PDCA-cyclus centraal staat.

T.a.v. kwaliteitsbeleid zijn de volgende verantwoordelijkheden vastgelegd:

De financieel directeur is voorzitter van het managementteam en er is een kwaliteitsmedewerker aangesteld voor het onderhouden en verbeteren van het kwaliteitsmanagementsysteem. Het management verzorgt samen met de kwaliteitsmedewerker het maken van analyses op het gebied van klanttevredenheid, interne auditing, en diensten, klantenklachten, corrigerende- en preventieve maatregelen. Deze analyses vinden minimaal jaarlijks plaats voorafgaand aan het management-review. De resultaten hiervan, alsmede de bijsturing van doelstellingen, worden in notulen opgenomen.

Het management heeft de verantwoordelijkheden en de bevoegdheid om zeker te stellen dat het kwaliteitsmanagementsysteem zoals omschreven in het kwaliteitshandboek wordt uitgevoerd en continu wordt verbeterd.

Iedere medewerker van Laurens & Nivard IT Services heeft de verantwoordelijkheid en de vrijheid om:

- Kwaliteitsproblemen te herkennen en te melden
- Oplossingen langs bestaande hiërarchische wegen te initiëren, aan te bevelen of aan te geven;
- De uitvoering van de gekozen oplossingen te controleren;
- Afwijkingen in het kwaliteitsmanagementsysteem te signaleren;

Informatiebeveiligingsbeleid

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 ervoor te zorgen dat:

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

geborgd zijn middels adequate preventieve maatregelen én processen en procedures bij beveiligingsincidenten.

T.a.v. informatiebeveiliging zijn de volgende verantwoordelijkheden vastgelegd:

1. De directie heeft dit Informatiebeveiligingsbeleid goedgekeurd;
2. 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 Information Security Manager.
3. 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.
4. Het naleven van informatiebeveiligingsprocedures zoals uiteengezet in de beleids- en richtlijnstukken wordt geaccepteerd als onderdeel van de standaardwerkwijzen binnen de organisatie. Niet-naleving leidt tot disciplinaire maatregelen.
5. Aan alle wettelijke en reglementaire vereisten wordt voldaan en regelmatig op wijzigingen gecontroleerd.
6. Er is een bedrijfscontinuïteitsplan. Dit wordt onderhouden, getest en regelmatig herzien.
7. Dit informatiebeveiligingsbeleid wordt regelmatig herzien en kan door de informatiebeveiligingsmanager worden gewijzigd om de blijvende levensvatbaarheid, toepasbaarheid en naleving van de wetgeving te waarborgen en om de informatiebeveiliging systemen voortdurend te verbeteren.
8. De directie stuurt erop aan dat er wordt voldaan aan de geldende wet- en regelgeving en dat middels het Informatiebeveiligingsmanagementsysteem continue verbetering wordt bewerkstelligd binnen de organisatie.

Plaats, datum	**Reeuwijk, 22 juni 2026**
Naam	**L.H.J. Slikkerveer**
Functie	**Financieel directeur**