****

**BELEIDSVERKLARING EN PROCEDURE**

**Clean Desk Beleid**

[ Voer hier uw bedrijfsnaam in ]

**Werkbeleidsnummer** Voer hier het beleidsnummer in

**Ingangsdatum:**

**Uitgegeven door:** Voer hier de naam in

**Goedgekeurd door** Voer hier de naam in

1. **DOEL**

Dit beleid wil [ Voer hier uw bedrijfsnaam in ] ondersteunen met het beheer van   
alle vertrouwelijke informatie via een *Clean Desk* Beleid dat in de hele organisatie   
wordt ingevoerd. Het biedt een duidelijk en uitgebreid inzicht in eisen voor informatiebeveiliging en lege bureaus.

Dit beleid wil verzekeren dat medewerkers van [ Voer hier uw bedrijfsnaam in ]:

* Wetten naleven met betrekking tot informatiebeveiliging en privacy;
* De dreiging van een beveiligingsincident helpen verminderen; en
* De vertrouwelijke informatie van onze klanten, ons bedrijf, onze stakeholders   
  en elkaar beschermen.

Implementatie en naleving van dit beleid is van wezenlijk belang voor de doeltreffendheid ervan. Onvolledige of selectieve implementatie kan [ Voer hier uw bedrijfsnaam in] blootstellen aan juridische risico's. Daarom moet elke medewerker   
het beleid begrijpen en meewerken aan de implementatie en naleving ervan.

**Beleidsbeheer** - neem bij vragen, opmerkingen of suggesties over dit beleid contact   
op met [ Voer hier de NAAM VAN DE CONTACTPERSOON EN DE TITEL in ].

1. **OMVANG**

Dit beleid is van toepassing op alle gedrukte documenten, openbare informatie en vertrouwelijke Informatie (zoals gedefinieerd in **Sectie 4.** hieronder) in eigendom van   
[ Voer hier uw bedrijfsnaam in ] of waarvan [ Voer hier uw bedrijfsnaam in ] een partij   
of ondertekenaar is.

1. **VERANTWOORDELIJKHEDEN**

**Senior management** moet ervoor zorgen dat dit beleid op alle bedrijfslocaties wordt gevolgd. Eén lid van het senior management wordt benoemd tot "Documentbeheerder" met onderstaande verantwoordelijkheden. Andere leden van het senior management zijn verantwoordelijk voor de toepassing van het beleid in hun verantwoordelijkheidsgebieden.

De rol van **Documentbeheerder** ("DB"), die momenteel is toegewezen aan de [ Voer   
de naam van de verantwoordelijke functie in ], moet de implementatie van dit beleid ondersteunen en leiden, en ervoor zorgen dat alle medewerkers zich ervan bewust   
zijn en training hebben gevolgd.

**Medewerkers** – Alle medewerkers van [ Voer hier uw bedrijfsnaam in ] zijn verantwoordelijk voor de naleving van dit beleid.

1. **DEFINITIES**

**4.1 Document** –Alle papieren stukken die informatie bevatten over [ Voer hier uw bedrijfsnaam in ], de eigenaars, medewerkers, dochterondernemingen, klanten, metgezellen, aannemers en zakelijke partners ervan.

**4.2 Vertrouwelijke Informatie** –Alle informatie die wordt geproduceerd tijdens de activiteiten van [ Voer hier uw bedrijfsnaam in ] die niet beschikbaar is in openbare bronnen, wordt beschouwd als vertrouwelijk. Doorgaans zijn alle documenten of bestanden met zakelijke gegevens, namen van klanten, partners of medewerkers, en prijsgegevens persoonlijke informatie. Dit omvat, maar is niet beperkt tot [ Voer hier SPECIFIEKE DOCUMENTTYPES in ]. Dit omvat ook informatie van individuen zoals gedefinieerd door gegevensbeschermingswetgeving, alsmede informatie die beschikbaar is voor ons bedrijf als gevolg van onze zakelijke praktijken, maar die niet algemeen bekend of op eenvoudige wijze verkrijgbaar is voor anderen buiten ons bedrijf, maar doorgaans in ons bedrijf kan worden gebruikt.

Documenten met vertrouwelijke informatie omvatten, maar zijn niet beperkt tot:

|  |  |
| --- | --- |
| Boekhoudkundige documenten  Documenten met betrekking tot informatietechnologie  Algemene contracten  Klantenlijsten  Interne rapporten  Loonadministratie  Trainingsinformatie en -handleidingen  Begrotingen op directieniveau  Klantencorrespondentie  Juridische contracten  Strategische rapporten  Gezondheids- en veiligheidsdossiers  Medische dossiers  Looninformatie | Juridische bedrijfsdossiers  Aankooporders van leveranciers  Leveranciersdossiers  Leveranciersspecificaties  Onderzoeks- en ontwikkelingsrapporten  Functioneringsgesprekken  Producttesten en resultaten  Productontwikkelingsplannen  Verkoop- en marketingrapporten  Specificaties en tekeningen  Interne communicatie  Reclamemateriaal  Zakelijke strategieën |

**4.3** **Openbare Informatie** – Documenten of informatie die niet worden beschouwd   
als vertrouwelijke informatie.

**4.4 Leeg Bureau** – De bureaus van alle medewerkers moeten zijn georganiseerd   
op een manier waarbij alleen materiaal dat momenteel wordt gebruikt of dat weldra zal worden gebruikt, zichtbaar is. Als een medewerker voor langere periode niet achter zijn/haar bureau zit, wordt openbare informatie netjes opgeborgen in mappen en moet strikt vertrouwelijke informatie afgesloten worden opgeborgen.

**4.5 DISCLAIMER - Juridische en Financiële Regelgeving** – In sommige rechtsgebieden en domeinen kunnen personeels-, juridische en financiële documenten onderworpen zijn aan specifieke regelgeving die voorschrijft hoe   
deze moeten worden bewaard, verspreid, opgeslagen en vernietigd. Neem   
contact op met de Documentbeheerder (“DB”) voor specifieke informatie,   
richtlijnen en praktijken met betrekking tot deze documenten in verband met   
dit *Clean Desk* Beleid.

**5. CLEAN DESK PROCEDURES**

Deze sectie beschrijft de clean desk procedures voor alle medewerkers en is van toepassing op alle soorten informatie die wordt vastgelegd door medewerkers, inclusief **Openbare, Vertrouwelijke Informatie** en **Algemene Zakelijke Informatie.**

**5.1 ONSITE** –Het *Clean Desk* Beleid van [ Voer hier uw bedrijfsnaam in ] vereist dat alle vertrouwelijke informatie op uw bureau buiten zicht moet worden opgeborgen als u voor langere tijd niet aanwezig bent. Bijvoorbeeld tijdens pauzes gedurende de werkdag moeten alle vertrouwelijke documenten worden opgeborgen in een afsluitbare archiefkast. Dit geldt voor zowel digitale informatie als papieren documenten. Computerschermen moeten zijn beveiligd met een wachtwoord   
en alle mobiele telefoons moeten afgesloten worden opgeborgen of te allen tijde   
in het bezit van de medewerker zijn. Het is de bedoeling dat afvalpapier of ongewenste papieren documenten in de veilige Shred-it recyclageconsoles   
worden geplaatst en niet in algemene vuilbakken of papiermanden.

**5.2 OFFSITE** – Het is de verantwoordelijkheid van elke medewerker van dit bedrijf,   
in overeenstemming met de gegevensbeschermingswetgeving, om de vertrouwelijke informatie van ons bedrijf en de medewerkers, partners en klanten ervan te beschermen. Vertrouwelijke informatie mag alleen mee naar huis worden genomen indien absoluut noodzakelijk. Als een medewerker thuis op een eigen computer bedrijfsbestanden opent en afdrukt, moeten alle computerbeveiligingssoftware up-to-date en effectief zijn. Papier dat thuis   
wordt geproduceerd en niet langer wordt gebruikt, moet op de werkplek worden vernietigd in de veilige Shred-it recyclageconsoles.