INVULLING GEVEN AAN FUNCTIE RISICOPROFIELEN

BIJLAGE BIJ BROCHURE KWETSBARE FUNCTIES

VOORBEELD: WERKGEBIEDEN (VET), TAKEN EN BEVOEGDHEDEN

Verlenen/ gunnen

- Het toekennen van toegangspassen tot een bedrijfsgebouw
- Machtigingen
- Geven van autorisaties tot bedrijfssoftware

Innen/ ontvangen

- Ontvangen van betalingen van klanten voor geleverde producten of diensten
- Incasseren van facturen
- Ontvangst van fondsenwervingen en donaties (bij non-profits)
- Heffingen en innen van belastingen
- Inning van lidgelden bij een ledenorganisatie
- Ontvangen van investeringen of subsidies
- Ontvangst van goederen en diensten van leveranciers bij leveringen

(Uit)besteden/ aankoop

- Aankoop van goederen zoals kantoormateriaal, softwarelicenties, marketingdiensten of machines
- Het plaatsen van orders en het geven van opdrachten aan leveranciers.
- Het inhuren van consultants of freelancers
- Het uitbesteden van IT-beheer aan een externe partij
- het gunnen van een aanbesteding aan een leverancier
- Het uitbesteden van logistiek aan een transportbedrijf

Uitkeren / toekennen

- Toekenning van eindejaarspremies aan medewerkers
- Verstrekking van subsidies aan partners of goede doelen
- Het toekennen van een leasewagen of een opleidingsbudget aan een werknemer
- Uitbetaling van salesbonussen

Beoordelen

- Evaluatiegesprekken met medewerkers
- Beoordelen van leveranciers op leverbetrouwbaarheid en prijs-kwaliteitverhouding
- Selectie en beoordeling van sollicitanten tijdens rekruteringsprocedures
- Auditresultaten beoordelen van interne processen

Handhaven

- Uitvoeren van interne controles op naleving van veiligheidsvoorschriften
- Handhaven van AVG-richtlijnen
- Opleggen van sancties bij schending van gedragscodes
- Controleren van declaraties
- Het nemen van sancties bij misbruik van bedrijfsmiddelen
- Het opleggen van boetes

Omgaan met informatie

- Omgaan met (gevoelige of vertrouwelijke) informatie
- Beheren van vertrouwelijke klantendata in een CRM-systeem
- Verantwoorde omgang met bedrijfslaptop en zakelijke telefoon waar (gevoelige) informatie op bewaard wordt
- Gegevensverwerking

Omgaan met middelen

- Correct gebruik van bedrijfswagen en tankkaart
- Beheren van onkosten en het opvolgen van budgetten binnen projecten of afdelingen
- Correcte onkostendeclaraties
- Geen ongepast gebruik van werkmiddelen zoals laptop, werk-gsm, internet

Contacten met derden

- Contacten met concullega's, klanten, leveranciers, buitenlandse partijen zoals bij onderhandelingen met leveranciers over prijzen en contractvoorwaarden
- Samenwerking met internationale partners bij joint ventures
- Klantencontact tijdens aftersales of klantenservice,
- Overleg met branchegenoten in een beroepsvereniging of op netwerkevents
- (internationale) Partijen die je benaderen

VOORBEELD: KWETSBAARHEDEN

Autonomie/solistisch handelen

- Veel discretionaire bevoegdheid
- Veel alleen beslissen en uitvoeren
- Veel thuiswerken etc.

Specialist/ sleutelfunctie

- Als enige over specialistische kennis beschikken
- Kennisconcentratie of etc.
- Alleen op een cruciaal /proceskritisch domein werken

Persoonlijkheidskenmerken en situatie van medewerker

- (Gok)verslaving,
- Financiële problemen
- Ontbreken van loopbaanperspectief
- Criminele contacten
- Gevoel onheus behandeld te zijn
- Veel belang hechten aan macht en status
- Bepaalde overtuigingen

Draaideurconstructies/ belangenvermenging

- Medewerkers die een nevenfunctie hebben die nauw aansluit bij hun functie in de organisatie
- (Ex-)medewerkers die terug als consultant/leverancier worden ingehuurd

Management/leiderschap

- Houding en (voorbeeld)gedrag management
- Tone at the top

Organisatiecultuur

- Competitiedrang
- Onrealistische verwachtingen
- Angstcultuur
- Bestaan van verschillende culturen naast elkaar
- Scherpe deadlines
- Druk door beursnotering
- Concurrentiedruk
- Slecht voorbeeldgedrag van de omgeving zoals van collega's

Complexiteit

- Ingewikkelde (juridische/fiscale) constructies
- Onduidelijke samenwerkingsverbanden
- Onoverzichtelijke (productie)keten

Verandering/dynamiek

- Sterke groei/krimp,
- Crisissituaties,
- Bezuiniging/reorganisatie
- Digitalisering
- Organisatorische verandering zoals fusie, overname, verhuizing, etc.
- Gebruik nieuwe technieken zoals AI
- Upscale van Start-up

Probleemhistorie

- Integriteitsincidenten
- Werkachterstand,

VOORBEELD: MAATREGELEN

Verlenen/ gunnen

- Autorisatiebeleid op basis van functie (need-to-access)
- Registratie en goedkeuring van elke toegangspas door bevoegde manager of HR
- Automatische deactivatie bij uitdiensttreding of na lange inactiviteit
- Toegangslogboeken en logging van bewegingen binnen gevoelige zones
- Beperkte toegang tot kritieke ruimtes (bijv. serverruimtes, archieven)
- Twee-factorverificatie voor gevoelige toegangen (pas met pincode of biometrie)
- Rechten per functie/proces
- Autorisatie-aanvraagprocedure met goedkeuring door verantwoordelijke manager én systeembeheerder
- Het ontvangen van geld digitaal laten verlopen
- Automatische koppeling tussen facturatie- en boekhoudsysteem
- Gebruik van unieke betaalkenmerken (zoals gestructureerde mededeling)
- Opleiding van personeel over fiscale regelgeving
- Functiescheiding tussen bv. bestellen en goedkeuren
- Periodieke review van toegangsrechten (bv. elk kwartaal)
- Logging en monitoring van kritieke handelingen in het systeem
- Directe intrekking van toegang bij functiewijziging of vertrek
- Gedocumenteerde en ondertekende volmachten/machtigingslijsten
- Autorisatiematrix gekoppeld aan functies, bedragen en processen
  Tweehandtekeningenprincipe bij hogere bedragen of risicovolle beslissingen
- Beheer van volmachten in een centraal register, met jaarlijkse controle
- Beperkingen in bank- of softwaresystemen die alleen toegelaten handelingen toestaan
- Gebruik van erkende betaalkanalen (bv. iDEAL, SEPA, creditcard met 2FA)
- Transparant donatieregister gekoppeld aan bankafschriften
- Transparante rapportage- en bezwaarprocedures

VOORBEELD: MAATREGELEN (VERVOLG)

Innen/ ontvangen

- Beperking van toegang tot rekeninginformatie (autorisatiebeheer)
- Afstemming van betalingen met openstaande facturen op dagelijkse basis
- Duidelijke subsidievoorwaarden vastleggen en opvolgen
- Scheiding van taken bij het aanvragen en registreren van subsidies
- Voorafgaande goedkeuring door bevoegde personen.
- Interne controle op subsidie-aanvragen versus ontvangen bedragen
- Periodieke controles door een onafhankelijke interne of externe auditor
- Gebruik van gevalideerde berekeningsmodellen/software
- Controle op actieve ledenstatus vóór inning
- Publicatie van jaarlijkse rapporten over besteding van fondsen
- Beperkte toegang tot donatiebeheer
- Afstemming tussen bestelling, leveringsbon en factuur
- Goederenontvangstcontrole (kwalitatief en kwantitatief)
- Gebruik van bestel- en ontvangstformulieren
- Enkel geautoriseerde leveranciers in het systeem
- Jaarlijkse herziening en goedkeuring van lidgelden
- Automatische facturatie en incasso gekoppeld aan ledenbeheer
- Ledenportaal voor inzage in status en betaling
- Medewerkers screenen op eventuele risico's

(Uit)besteden/ aankoop

- Rode vlaggen in betalingssysteem invoeren bij ongebruiklelijke transacties
- Schriftelijke verklaring van belangen om belangenvermenging tegen te gaan
- Budgetcontrole vóór bestelling (goedkeuringsworkflow)
- Gebruik van een geautoriseerde leverancierslijst
- Procedure voor het openen van offertes met meerdere medewerkers
- Scheiding van functies van aanvrager, goedkeurder en ontvanger
- Controle op bestelbon vs. leveringsbon vs. factuur
- Offertevergelijking bij aankopen boven drempelbedrag
- Registratie van bestellingen in een centraal systeem
- Formele bestelprocedure verplicht voor alle aankopen
- Autorisatiematrix voor goedkeuring van orders
- Transparante leveranciersselectie en documentatie van motivatie
- Controle op dubbele bestellingen via bestelhistoriek
- Duidelijke SLA's (Service Level Agreements) met meetbare KPI's
- Beveiligings- en privacyclausules in het contract
- Gebruik van raamcontracten waar mogelijk
- Regelmatige evaluatie en audit van (IT-)leverancier
- Beperking van toegang tot kritieke systemen (principle of least privilege)
- Escrow-afspraken voor software/ code bij faillissement
- Opstellen van duidelijke opdrachtomschrijvingen en resultaten
- Tarieven vergelijken met marktstandaarden of benchmarks
- Beperking van contractduur en uitgaven zonder verlenging
- Voorafgaande goedkeuring door bevoegde manager/directie
- Controle op dubbele dienstverbanden of belangenconflicten
- Strikte naleving van aanbestedingswetgeving (openbaar, onderhands, EU-drempel...)
- Transparante beoordelingscriteria vooraf bekendgemaakt
- Commissie met meerdere leden voor beoordeling
- Informatie-afscherming tussen inschrijvers en besluitvormers
- Documentatie en archivering van hele procedure
- Track en trace systemen om leveringen te volgen

Uitkeren / toekennen

- Duidelijke beleidsregels en criteria vastgelegd in cao, arbeidsreglement of beleid
- Automatische berekening via loonadministratiesysteem, gekoppeld aan HR-gegevens
- Goedkeuring door HR of directie vóór uitbetaling
- Scheiding van taken tussen berekening, goedkeuring en betaling
- Transparante bonusstructuur op basis van meetbare en geverifieerde prestaties
- Controlemomenten door management of finance vóór goedkeuring
- Beoordeling door een onafhankelijke commissie (i.p.v. één persoon)
- Bedrijfswagenbeleid met duidelijke toekenningsvoorwaarden (functieniveau, km-vergoeding, privégebruik...)
- Controle op facturen en bewijs van deelname/certificaat
- Subsidieovereenkomst met resultaats- of rapportageverplichting
- Formele aanvraagprocedure met documentatieverplichting
- Goedkeuringsprocedure door HR of wagenparkbeheerder

VOORBEELD: MAATREGELEN (VERVOLG)

Uitkeren / toekennen (vervolg)

- Steekproefcontrole op juistheid en volledigheid
- Vastlegging van bonussen in schriftelijke overeenkomsten
- Controle op dubbele of foutieve toekenningen via loonverwerking
- Registratie van bonusberekening en onderbouwing in dossier
- Controle op rechtspersoonlijkheid, betrouwbaarheid en doelbesteding van de ontvanger
- Opvolging via een leerportaal of HR-tool
- Afsluiten van een opleidings- of terugbetalingsclausule bij duurdere opleidingen
- Medewerkers screenen op eventuele risico's
- Gebruik van standaardcontracten met vermelding van rechten en plichten
- Registratie in HR-systeem met koppeling aan loonfiche
- Jaarlijkse herziening van wagengebruik en bijtelling
- Opleidingsbeleid met objectieve criteria (bv. functie, ontwikkelplan)
- Voorafgaande goedkeuring door leidinggevende of HR
- Duidelijke selectiecriteria en subsidievoorwaarden publiceren

Beoordelen

- Gestandaardiseerde evaluatieformulieren en competentiemodellen
- Training voor leidinggevenden over objectief en constructief evalueren
- Vier-ogen-principe (HR of hogere manager kijkt evaluaties na)
- Duidelijke afspraken over doelstellingen (SMART) aan het begin van het jaar
- Mogelijkheid tot bezwaar of feedback van werknemer in het evaluatieverslag
- Gebruik van scorekaarten (vendor rating) met automatische rapportage
- Documentatie van beoordeling en herzieningsmomenten
- Rotatie of hertest bij vaste leveranciers na X jaar
- Competentiegericht interviewen met gestandaardiseerde vragen
- Scoreformulieren per kandidaat op basis van vooraf bepaalde criteria
- Minstens twee beoordelaars per sollicitatiegesprek
- Objectieve beoordelingscriteria vastleggen (bijvoorbeeld leverbetrouwbaarheid, kwaliteit, prijs, service)
- Beperkte toegang tot evaluatiedossiers (HR-privacy
- Periodieke leveranciersbeoordeling op basis van meetbare data
- Input van verschillende afdelingen (bv. logistiek + aankoop + productie)
- Bewustwordingstraining rond bias en inclusie voor recruiters
- Beoordeling van auditrapporten door onafhankelijke personen of comité
- Opvolgplan verplicht bij elk auditrapport, met deadlines en verantwoordelijken
- Transparante rapportering naar directie of auditcomité
- Risk-based benadering bij beoordeling van auditbevindingen
- Her-audit of controle van verbetermaatregelen binnen 6 tot 12 maanden
- Gebruik van auditsoftware of trackingtools voor opvolging
- Objectieve selectieprocedures met testcases of assessments
- Bewaring van selectieverslagen als onderbouwing van keuze

Handhaven

- Voorafgaande goedkeuring bij hoge bedragen of uitzonderingen
- Controle door administratie of boekhouding op bonnen, data, reden
- Analyse van uitgavenpatronen voor detectie van misbruik
- Herinnering aan gebruiksregels via intranet of onboarding
- Proportionele sanctieladder: waarschuwing, daarna terugvordering, ten slotte boete/HR-maatregel
- Objectieve en gedocumenteerde vaststelling van de overtreding
- Dataregister bijhouden van alle verwerkingen
- Hoor- en wederhoorprincipe vóór het opleggen van een boete
- Interne richtlijnen voor proportionele sancties
- Interne escalatieprocedure of bezwaarprocedure beschikbaar stellen
- Registratie van opgelegde boetes en opvolging van herhaling
- Regelmatig functieroulatie zodat medewerkers niet te lang in dezelfde of in de eigen regio werken
- Regelmatige veiligheidsaudits en werkplekinspecties
- Actuele risicoanalyses en preventieplannen
- Schriftelijke procedures (bv. toolbox meetings) en zichtbare veiligheidsinstructies
- Training en herhalingstrainingen voor medewerkers
- Boeteclausules opnemen in contracten met duidelijke voorwaarden
- Privacy by design in systemen en processen
- Regelmatige herhaling via e-learning of workshops
- Registratie van incidenten en near-misses met opvolging
- Toegangscontrole tot risicovolle zones enkel voor opgeleide personen
- Heldere gedragscode met voorbeelden en grensoverschrijdend gedrag

VOORBEELD: MAATREGELEN (VERVOLG)

Handhaven (vervolg)

- Trainingen over ethisch gedrag en integriteit
- Verplichte DPA-overeenkomsten met externe verwerkers
- Training voor medewerkers over privacybewust handelen
- Duidelijk declaratiebeleid met toegestane en verboden uitgaven
- Toegangscontrole tot persoonsgegevens (need-to-know)
- Klokkenluidersregeling
- Bekendmaking en ondertekening van gedragscode bij indiensttreding
- Vertrouwelijk meldpunt
- Objectieve sanctieprocedure met hoor- en wederhoor
- Duidelijke bewaartermijnen en automatische gegevensverwijdering

Omgaan met informatie

- Classificatie van informatie (openbaar / intern / vertrouwelijk / geheim)
- Beleid voor omgaan met vertrouwelijke documenten (versleuteling, vernietiging, geen onbeheerde papieren)
- Training over informatiebeveiliging en vertrouwelijkheid
- Toegangsrechten beperken op basis van functie (“need to know”)
- Verbod op privé-opslag of delen via onbeveiligde kanalen (bv. persoonlijke e-mail)
- Geheimhoudingsverklaring bij indiensttreding of samenwerking
- Duidelijke verwerkingsinstructies per proces (verzameling, opslag, gebruik, verwijderen)
- Toestemming en rechtmatigheid van verwerking altijd controleren (conform AVG)
- Technische maatregelen zoals versleuteling, pseudonimisering, firewalls
- Verwerkersovereenkomsten afsluiten met externe partijen
- Privacy Impact Assessments bij risicovolle verwerkingen
- Audit trails activeren voor gevoelige gegevensbewerkingen
- Loggen van activiteiten en periodieke controle op CRM-gebruik
- Beperking op export/download van data
- Regelmatige opschoning en controle op verouderde of onjuiste gegevens
- Beveiligingsbeleid voor apparaten (bv. automatisch vergrendelen, versleutelde harde schijf)
- Gebruik van Mobile Device Management (MDM) voor controle op instellingen, apps en op afstand wissen
- Geen privégebruik of installatie van niet-goedgekeurde software/apps
- Verplichte antivirus, VPN en firewall op alle apparaten
- Instructies bij verlies of diefstal (onmiddellijk melden, blokkeren op afstand)
- Regelmatige controle op updates en patches door IT
- Multifactor authenticatie
- Verplichte training in CRM-gebruik en dataveiligheid
- Role-based access control (alleen toegang tot relevante data)

Omgaan met middelen

- Maandelijkse controle op tankbeurten (locatie, hoeveelheid, type brandstof)
- Tracking van kilometers of black box (indien toegelaten)
- Meldplicht voor schade, boetes en ongevallen
- Beperkingen op tankkaart (geen shopaankopen, limiet per dag/week)
- Vastgelegde project- of afdelingsbudgetten met goedkeuring vooraf
- Real-time budgetopvolging via dashboards of ERP-software
- Verplichte budgetcontrole vóór grote uitgaven
- Periodieke rapportage aan verantwoordelijke managers
- Onkostenbeleid met duidelijke limieten, toegestane kosten en verplichte bewijsstukken
- Gebruik van declaratiesoftware met automatische controles (datum, duplicaten, btw, limieten)
- Logging en monitoring van ongebruikelijke IT-activiteit (met inachtneming van privacyregels)
- Bij verlies of fout gebruik: meldplicht en opvolging door IT of HR
- Kluisprocedure voor wie met contant geld werkt
- Bedrijfswagenbeleid met regels rond gebruik, onderhoud, boetes, tankkaart, privégebruik
- Bewijs van ontvangst van werkmateriaal bijvoorbeeld ondertekening bij ontvangst van wagen en kaart
- Alarmmeldingen bij overschrijdingen of afwijkingen
- Toewijzing van één budgethouder per afdeling/project
- Goedkeuringsflow met functiescheiding
- Verplichte indiening binnen een bepaalde termijn (bv. 30 dagen)
- Steekproeven of audit door finance
- Consequenties bij misbruik duidelijk communiceren
- ICT-gebruiksbeleid met richtlijnen voor zakelijk vs. beperkt privégebruik
- Blokkeren van risicovolle websites of apps via netwerkbeheer
- Training over cyberveilig gedrag en social engineering
- Verplicht gebruik van VPN, antivirus en schermvergrendeling

VOORBEELD: MAATREGELEN (VERVOLG)

Contacten met derden

- Verklaring van medewerkers over welke directe en indirecte banden ze hebben
- Training over mededingingsrecht (kartelverboden, informatie-uitwisseling)
- Afspraken voor netwerkevents en branchebijeenkomsten
- Vooraf toestemming of briefings bij deelname aan formele overleggen
- Verbod op delen van concurrentiegevoelige info (prijzen, volumes, strategie)
- Mogelijkheid tot rapporteren van ongepast contact of voorstellen
- Due diligence op internationale partners (KYC, sanctielijsten, reputatiecheck)
- Gebruik van standaardcontracten met clausules over anti-corruptie, exportregels, ethiek
- Training in exportcontrole, anti-corruptie en culturele sensitiviteit
- Geen contante betalingen of “facilitating payments” (smeergeld)
- Verplicht overleg met juridische of compliance-afdeling bij twijfel of onderhandelingen
- Duidelijke richtlijnen en scripts voor communicatie met klanten
- Training in herkennen van social engineering of valse voorstellen
- Training in klantgericht, juridisch correct en empathisch handelen
- Toegang tot klantdata beperken tot wat nodig is
- Monitoring van klachtenafhandeling en klanttevredenheid
- Escalatieprocedure bij moeilijke of grensoverschrijdende situaties
- Autorisatiebeleid: alleen bevoegde personen mogen onderhandelen/tekenen
- Aanwezigheid van twee medewerkers bij cruciale onderhandelingen
- Vastleggen van alle stappen en afspraken schriftelijk (in e-mail of notulen)
- Beoordeling van contracten door juridische dienst
- Gedragscode over omgang met leveranciers (bv. geen giften, transparantie)
- Controle op herkomst van contact (domein, afzender, IP)
- Gebruik van whitelist/blacklist van vertrouwde externe contacten
- Verplichte screening van buitenlandse investeerders of partners
- Geen informatie delen of contracten aangaan zonder interne afstemming
- Screening van medewerkers