|  |
| --- |
| Template Human ResourceOndertitel |

|  |  |
| --- | --- |
| Auteur(s): |  |
| Versie: |  |
| Datum: | Kies of typ een datum |
| Kenmerk: |  |
|  |
|  |

**Documentinformatie**

Dit document maakt onderdeel uit van een complete set (piramide) met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Dit document heeft betrekking op de laag Thema-beleid in de beleidspiramide.



**Versiebeheer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Verwerking** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Distributielijst**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Ontvanger** | **Doel** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Vastgesteld door** | **Vastgesteld op** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Samenhang met andere documenten**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Bovenliggend** | **Gelijk niveau** | **Onderliggend** |
| [INFORMATIEBEVEILIGINGSBELEID] | x |  |  |
| [HR BELEID – GENERIEK] | x |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | HR.01; HR.02; HR.03; HR.04; HR05; HR.06 |
| ISO27001 | A.6 |

**Creative Commons**

Dit template is een product van het SURF Security Expertise Centrum en beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal. <https://creativecommons.org/licenses/by/4.0/deed.nl>

Inhoudsopgave

|  |
| --- |
| [Samenvatting 4](#_Toc160692289)[1 Inleiding 5](#_Toc160692290)[2 Instroom 6](#_Toc160692291)[3 Training, certificering en opleiding 7](#_Toc160692292)[4 Afhankelijkheid van individuele medewerkers 8](#_Toc160692293)[5 Doorstroom en Uitstroom 9](#_Toc160692294)[6 Kennisdelen 10](#_Toc160692295)[7 Awareness 11](#_Toc160692296)[Vaststelling 12](#_Toc160692297)[Bijlage 1 Achtergrondscontrole- en doorlichtingscriteria per functieniveau 13](#_Toc160692298)[1.1 Operationeel niveau 13](#_Toc160692299)[1.2 Technisch niveau 13](#_Toc160692300)[1.3 Leidinggevend niveau 13](#_Toc160692301)[1.4 Strategisch niveau 13](#_Toc160692302) |

Samenvatting

Hier komt een samenvatting, op zichzelf leesbaar, van de inhoud van dit document in max. 1 A4.

# Inleiding

Dit document geeft een overzicht van de processen en procedures voor informatiebeveiliging waar de [HR-AFDELING] een of meer taken in heeft.

Er zijn heldere procedures voor instroom, doorstroom en uitstroom van personeel. Bij werving en selectie van personeel is aandacht voor het screenen van het personeel. Nieuw personeel wordt getraind op het gebied van informatiebeveiliging en privacy. Er is aandacht voor bewustzijn op het gebied van informatiebeveiliging en privacy gedurende het gehele dienstverband.

# Instroom

Bij het aannemen van vaste en tijdelijke medewerkers worden vastgelegde procedures gevolgd die passen binnen de algemene instroomprocedures. Deze betreffen het indienst­tredingsproces, de zorg voor een positieve werksfeer en de introductie tot de werkplek en functie.

[INSTELLING] zorgt voor het in dienst hebben en houden van voldoende gekwalificeerde medewerkers die in staat zijn en worden gesteld hun respectievelijke vereiste en gewenste bijdragen te leveren aan de informatiebeveiliging van [INSTELLING].

[*Aan deze alinea kun je een aantal details toevoegen, als die zo zijn afgesproken. Denk bijvoorbeeld aan het bijhouden van overzichten van gevolgde cursussen en dergelijke. Dan weet je wat je in huis hebt, of mist. Of, als dat niet ergens anders is geregeld, vul dan hier aan met een paar regels over functieprofielen en minimumvereisten voor kandidaten. (Let wel op dat dit geen afvink-lijstje wordt, dat leidt in de praktijk vaak tot collega’s die wel de juiste vinkjes hebben, maar waarmee bijvoorbeeld niet goed valt samen te werken.). Kijk wel goed wie waarvoor verantwoordelijk is, je wilt niet in andermans vaarwater zitten.]*

In het aannameproces zijn doorlichtingen en achtergrondcontroles (screening) van kandidaten onderdeel van het proces.

De reikwijdte en diepgang van de (periodiek herhaalde) doorlichtingen en achtergrondcontroles is afhankelijk van de gevoeligheid en het kritieke gehalte van de respectievelijke functies voor de informatiebeveiliging van [INSTELLING]. In Bijlage 1 is een nadere specificatie opgenomen.

De doorlichtingen en achtergrondchecks gelden voor eigen medewerkers, ingehuurde krachten en (diensten)leveranciers.

Studenten zullen bij instroom worden gewezen op hun bijdrage aan de informatiebeveiliging van [INSTELLING].

Alle aannameprocessen en -procedures zijn goedgekeurd door [HET COLLEGE / DE RAAD VAN BESTUUR].

[*De hier genoemde punten zijn vereisten voor Volwassenheid 3. Zorg er dus beter voor dat je weet wie of waar (bij HR en/of de leidinggevenden?) dit op het bordje ligt, in de RACI-tabel én tussen de oren bij die collega’s. Auditors zullen ook evidence vragen, dus een mondelinge check zal niet genoeg zijn...]*

# Training, certificering en opleiding

[INSTELLING] heeft processen die ervoor zorgen dat medewerkers zijn getraind en opgeleid voor de informatiebeveiligingsaspecten in hun respectievelijke functies. Hierbij moet specifiek aandacht zijn voor medewerkers in ICT, Security, Privacy en functioneel-beheer functies of rollen.

[INSTELLING] stelt in elk geval verplicht aan nieuwe medewerkers dat zij binnen [één] maand na indiensttreding de verplichte opleidingen succesvol hebben doorlopen en waar nodig met afleggen van een kennistoets:

* Elearning Informatiebeveiliging binnen [INSTELLING]
* Elearning privacy binnen [INSTELLING]
* Elearning Gedragsregels ICT binnen [INSTELLING]

Bestaande medewerkers worden geacht verplicht nieuwe / opfris modules over deze thema's te volgen en af te ronden.

Medewerkers hebben individuele ontwikkelplannen (POP) waarmee hun kennis en kunde over o.a. informatiebeveiliging wordt geactualiseerd en/of uitgebreid, en voeren die aantoonbaar uit.

Periodiek wordt geverifieerd of medewerkers door middel van opleiding, training en/of opgedane ervaring (nog) de informatiebeveiligingscompetenties hebben die nodig zijn voor hun respectievelijke functies.

De processen voor training, certificering en opleiding van medewerkers in de informatiebeveiligingsaspecten van hun respectievelijke functies zijn goedgekeurd door [HR / DIRECTIE / MANAGEMENT / OF] de leidinggevenden van betreffende afdelingen.

[*De hiervoor beschreven punten zijn (ook) toetspunten voor Volwassenheidsniveau 3. Zorg er dus beter voor dat je a. weet wie of waar (bij HR en/of de leidinggevenden?) dit op het bordje ligt, b. dat er daadwerkelijk POPs en kennis/ervaringsoverzichten zijn.]*

# Afhankelijkheid van individuele medewerkers

Door planning van opvolging in de bezetting van functies, proefdraaien met het vervangen van collega’s en het voorbereid hebben van collega’s op onderling elkaar tijdelijk of permanent moeten vervangen, voorkomt [INSTELLING] afhankelijkheid van individuele medewerkers voor de uitvoering van informatiebeveiligingstaken.

Deze drie aspecten zijn vast onderdeel van het trainingsprogramma voor alle [of benoem hier de specifieke sleutelposities] medewerkers.

Alle sleutelposities voor informatiebeveiliging zijn specifiek als zodanig benoemd en erkend door leidinggevenden.

[*Deze punten zijn (ook) toetspunten voor Volwassenheidsniveau 3. Zorg er dus voor dat je a. weet wie of waar (bij HR en/of de leidinggevenden?) dit op het bordje ligt, b. dit kan aantonen bijvoorbeeld door een lijstje van belangrijke functies met namen en de namen van back-ups, een overzicht van het trainingsprogramma.]*

# Doorstroom en Uitstroom

[INSTELLING] hanteert vaste procedures om de kennis van medewerkers die van functie veranderen of [INSTELLING] verlaten, over te dragen op opvolgende medewerkers.

[INSTELLING] hanteert vaste procedures om de toegangsrechten van medewerkers die van functie veranderen of [INSTELLING] verlaten, in te trekken en opnieuw uit te geven.

De kennisoverdracht en aanpassing van toegangsrechten gebeurt gelijk opgaand met de overdracht van de functie zodat informatiebeveiligingsrisico’s en continuïteitsrisico’s voor de functie-uitoefening minimaal zijn.

De procedures voor kennisoverdracht en wijzigingen in toegangsrechten zijn vastgelegd.

[*Deze punten zijn (ook) toetspunten voor Volwassenheidsniveau 3. Zorg er dus voor dat je a. weet wie of waar (bij HR en/of de leidinggevenden?) dit op het bordje ligt, b. dit kan aantonen.]*

# Kennisdelen

[INSTELLING] hanteert organisatie brede procedures voor kennisoverdracht en onderhoudt documentatie van systemen (waaronder training- en implementatiebeschrijvingen) op een niveau dat adequate ondersteuning van de organisatieprocessen mogelijk maakt. Dit betreft kennis en documentatie zowel voor eindgebruikers als voor operationele en technische ondersteuning.

[*Deze punten zijn (ook) toetspunten voor Volwassenheidsniveau 3. Zorg er dus voor dat je a. weet wie of waar (bij HR en/of de leidinggevenden?) dit op het bordje ligt, b. dit kan aantonen. Let op dat auditors misschien niet tevreden zijn met ‘een paar voorbeelden’ maar willen weten hoe je weet/aantoont dat de docu een beetje volledig is.]*

# Awareness

Door awareness-verhogende activiteiten wordt eenieder herinnerd aan hun rol in het grotere geheel van informatiebeveiliging. Om die goed te kunnen vervullen, is het nodig dat de awareness-verhogende activiteiten:

* Aansluiten bij de respectievelijke functies van medewerkers, studenten en andere betrokkenen;
* Aandacht geven aan kennis, houding en gedrag ten aanzien van informatiebeveiliging en de door ons gehanteerde regels en afspraken.

Omdat awareness-activiteiten betrekking hebben op medewerkers en andere personen, overlegt de [VOOR AWARENESS VERANTWOORDELIJKE FUNCTIONARIS] met [HR] over de planning, vorm en inhoud van de awareness-verhogende activiteiten.

Voor de awareness-verhogende activiteiten wordt gebruik gemaakt van diverse middelen. De [VOOR AWARENESS VERANTWOORDELIJKE FUNCTIONARIS] overlegt met [HR] over de optimale inzet van deze middelen.

Voor de activiteiten wordt gebruik gemaakt van een (jaar)planning, waarin de doelgroepen, onderwerpen en middelen afwisselend worden benaderd, aandacht gegeven c.q. ingezet.

# Vaststelling

Dit beleid is aldus vastgesteld.

[PLAATS], [DATUM].

[CISO / DIR IT / CIO].

[Na (her)vaststelling, ook de tabel op p.2 bijwerken]

1. Achtergrondscontrole- en doorlichtingscriteria per functieniveau

Achtergrondcontroles en doorlichtingen zijn cruciale elementen van het personeelsbeleid met betrekking tot informatiebeveiliging binnen [INSTELLING]. Het niveau van de controle en doorlichting kan variëren afhankelijk van de gevoeligheid en het kritieke gehalte van de functie voor de informatiebeveiliging van de organisatie.

Hieronder volgen de specifieke criteria per functieniveau.

* 1. Operationeel niveau

Voorbeeld functies op dit niveau zijn:

* Helpdeskmedewerker
* Systeembeheerder (niet-kritieke systemen)
* Administratief medewerkers

Criteria:

* Standaard achtergrondcontrole, inclusief controle van identiteit en referenties.
	1. Technisch niveau

Voorbeeld functies op dit niveau zijn:

* Netwerkbeheerder
* Applicatieontwikkelaar
* Databasebeheerder

Criteria:

* Uitgebreide achtergrondcontrole, inclusief controle van identiteit, referenties en werkverleden.
* Controle van eventuele certificeringen en opleidingen relevant voor de functie.
	1. Leidinggevend niveau

Voorbeeld functies op dit niveau zijn:

* IT-Manager
* Teamleider ICT
* Security Officer

Criteria:

* Diepgaande achtergrondcontrole, inclusief controle van identiteit, referenties, werkverleden en justitiële antecedenten.
* Controle van eventuele certificeringen, opleidingen en ervaring op het gebied van informatiebeveiliging.
* Screening op financiële geschiedenis eventuele conflicterende belangen.
	1. Strategisch niveau

Voorbeeld functies op dit niveau zijn:

* Chief Information Officer (CIO)
* Chief Information Security Officer (CISO)
* Hoofd IT-beveiliging

Criteria:

* Zeer grondige achtergrondcontrole, inclusief controle van identiteit, referenties, werkverleden, justitiële antecedenten en financiële geschiedenis.
* Uitgebreide screening op eventuele conflicterende belangen en contacten.
* Controle van certificeringen, opleidingen en ruime ervaring op het gebied van informatiebeveiliging en risicomanagement.

Deze criteria dienen als leidraad voor het bepalen van de reikwijdte en diepgang van de achtergrondcontroles en doorlichtingen voor verschillende functieniveaus binnen [INSTELLING]. Het is belangrijk om deze criteria regelmatig te evalueren en bij te werken om te blijven voldoen aan de behoeften van de organisatie en de vereisten voor informatiebeveiliging.