Normkader

- In onderstaande tabel is het normkader Digitale Ondermijning (NDO) opgenomen. De in blauw weergegeven tekstdelen zijn ondermijningspecifiek. De overige tekstdelen zijn bestaande CYRA-tekstdelen waarop het NDO aanhaakt.
- In het geval van beheersmaatregelen waarop het NDO een toevoeging doet op bestaande CYRA-beheersmaatregelen, wordt deze aanvulling in de tabel in blauw weergegeven onder “Ondermijningspecifieke beheersmaatregel”. De referentie in de eerste kolom verwijst dan naar het corresponderende normelement in de onderliggende norm ISO 27001:2022. In het geval de beheersmaatregel niet verwijst naar ISO 27001, is de tekst in zijn geheel blauw weergegeven. De referentie in de eerste kolom verwijst dan naar een NDO-eigen nummering.

Ref.	Beheersmaatregel en initiële vraag	Ad hoc	Best effort	Defined
5.1	**Beleidsregels voor informatiebeveiliging en privacy** Heeft de organisatie actuele beleidsregels omtrent informatiebeveiliging en privacy?	Hoewel er eventuele enkele beleidslijnen zijn, is er vooral sprake van een gangbare praktijk van handelen die niet op beleid gebaseerd is. **Ondermijningspecifieke beheersmaatregel:** Algemeen geldende ondermijningsrisico’s zijn bekend. Er is een procedure opgesteld voor het melden van potentiële ondermijningsignalen, het principe ‘least privilege’ wordt gehanteerd en gedragsregels zijn gecommuniceerd.	Het beleid is niet formeel goedgekeurd. Er is beleid op hoofdlijnen gepubliceerd met doelstellingen en uitgangspunten. Verantwoordelijkheden zijn toegekend en processen voor het behandelen van afwijkingen en uitzonderingen zijn bepaald. Het beleid op hoofdlijnen is nader uitgewerkt in onderwerp specifieke beleidsregels die de implementatie van beheersmaatregelen voor informatiebeveiliging en privacy verplicht stellen. **Ondermijningspecifieke beheersmaatregel:** Er is onderwerp specifiek beleid uitgewerkt voor: - Social media - BYOD (Bring Your Own Device) - Least privilege	Het gepubliceerde beleid op hoofdlijnen (zie L2) is goedgekeurd door de directie en tevens gecommuniceerd aan medewerkers en relevante externe partijen. Het beleid wordt periodiek beoordeeld op actualiteit én wanneer er zich een ernstig incident voordoet.
5.7	**Informatie en analyse over dreigingen** Wordt er gekeken naar bedreigingen op het gebied van informatiebeveiliging?	Er wordt rekening gehouden met mogelijke bedreigingen rond informatiebeveiliging. **Ondermijningspecifieke beheersmaatregel:** De organisatie houdt rekening met mogelijke bedreigingen die vanuit de eigen organisatie komen (‘insider threats’) gericht op misbruik van werkprocessen en informatie van de organisatie (of haar ketenpartners)	Mogelijke bedreigingen van de informatiebeveiliging van de organisatie worden in de gaten gehouden en hier wordt lering uit getrokken. **Ondermijningspecifieke beheersmaatregel:** Er zijn maatregelen getroffen die onbedoelde en/of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	Mogelijke bedreigingen rond informatiebeveiliging van de organisatie worden in de gaten gehouden. Deze worden verzameld en geanalyseerd om de kans dat zich een dergelijke situatie voor zal doen te verkleinen of om de mogelijke impact te verkleinen. Hierbij wordt rekening gehouden met het soort aanvallen, type aanvallers als ook welke methodes, tools en indicatoren gebruikt (kunnen) worden om een aanval te signaleren. **Ondermijningspecifieke beheersmaatregel:** De organisatie heeft beleid opgesteld ten aanzien van het delen van bedreigingsinformatie met andere organisaties.
5.9	**Inventarisatie van informatie en andere samenhangende bedrijfsmiddelen** Worden de met informatie samenhangende bedrijfsmiddelen vastgelegd?	Enkele bedrijfsmiddelen zijn in een overzicht opgenomen dat (ad hoc) actueel wordt gehouden. **Ondermijningspecifieke beheersmaatregel:** Bedrijfsmiddelen die vanuit het oogpunt van insider threat van belang zijn, waaronder in ieder geval persoonsgegevens bevattende bedrijfsmiddelen, zijn in een overzicht opgenomen dat jaarlijks wordt geactualiseerd.	Geïdentificeerde bedrijfsmiddelen zijn gekoppeld aan persoonlijke accounts en de inventaris wordt actueel gehouden. **Ondermijningspecifieke beheersmaatregel:** Werknemers zijn betrokken bij het identificeren van de ondermijningsrisico’s in verband met de bedrijfsmiddel(en).	Alle voor de levenscyclus van informatie relevante bedrijfsmiddelen zijn geïdentificeerd en worden in een inventarislijst onderhouden, gekoppeld aan persoonlijke accounts per (categorie van) bedrijfsmiddel(en). De inventaris wordt structureel actueel gehouden. **Ondermijningspecifieke beheersmaatregel:** De inventarisatie van bedrijfsmiddelen wordt jaarlijks beoordeeld aan de hand van de classificatie(s) van de bedrijfsmiddel(en) en hierbij wordt ondermijning specifiek in de risicoanalyse meegenomen.
5.12	**Classificatie van informatie** Hanteert de organisatie een classificatiemechanisme?	Informatie en de bedrijfsmiddelen waarin die is opgeslagen of anderszins wordt verwerkt, wordt/worden (deels) geclassificeerd. Ten behoeve hiervan wordt een classificatieschema gehanteerd met verschillende uniek benoemde niveaus. **Ondermijningspecifieke beheersmaatregel:** Het classificatieschema is gekoppeld aan tenminste de vertrouwelijkheid van informatie.	Informatie en de bedrijfsmiddelen waarin die is opgeslagen of anderszins wordt verwerkt, wordt/worden geclassificeerd en zijn voorzien van bijbehorende beheersmaatregelen per niveau. Eigenaren van bedrijfsmiddelen zijn verantwoordelijk voor de classificatie ervan. Het classificatieschema omvat regels voor classificatie en criteria voor herbeoordeling. Classificatie is opgenomen in procedures van de organisatie en is in overeenstemming met toegangsbeveiliging.	Informatie is geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.

Ref.	Beheersmaatregel en initiële vraag	Ad hoc	Best effort	Defined
NDO 1	**Screening** Wordt de achtergrond van personeel geverifieerd?	Het personeel, met inbegrip van voltijd-, deeltijd en tijdelijk personeel wordt ad hoc gescreend. Selectie van personeel vindt plaats o.b.v. een 4-ogen principe. Screening van open bronnen (waaronder social media) is onderdeel van een sollicitatieprocedure en wordt o.a. in de vacaturetekst gecommuniceerd. In ieder geval heeft de organisatie voor elke functiegroep binnen de organisatie in kaart gebracht welke risico's op ondermijning een rol spelen.	Er is een recruitmentproces voor (IT)personeel vastgesteld en geïmplementeerd waarin bedrijfseisen zijn opgenomen. Verificatie van de achtergrond kan plaatsvinden, maar is niet geformaliseerd. Indien personeel via dienstverleners wordt ingehuurd, worden screeningseisen opgenomen in vastgelegde afspraken tussen de organisatie en de dienstverleners. Er is een proces voor periodieke screening vastgesteld waarin controles op het gebruik van open bronnen en wijzigingen in persoonlijke omstandigheden zijn opgenomen in het kader van de inschatting van het risico op ondermijning.	De achtergrond van alle kandidaten voor een dienstverband wordt gecontroleerd voordat zij in dienst treden en daarna op gezette tijden herhaald. Controle staat in verhouding tot de bedrijfseisen, de classificatie van informatie waartoe toegang wordt verleend en de vastgestelde risico's. De screening is mede gebaseerd op ondermijningsrisico Bij aanstelling van nieuw personeel is er een formele procedure vastgesteld waarbij opgegeven referenties, trainingen en opleidingen van (op zijn minst) de afgelopen vijf jaar worden gevalideerd.
6.3	**Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging** Wordt kennis van het personeel op peil gebracht/gehouden?	Training en opleiding vindt op ad hoc basis plaats. Er is (vrijwel) geen sprake van persoonlijke certificering. **Ondermijningspecifieke beheersmaatregel:** De organisatie herinnert het personeel elk half jaar op het bestaan van de voorziening voor het melden van mogelijke (ondermijnings)signalen en de verplichting om deze verdachte activiteiten te melden. De organisatie geeft daarbij voorbeelden van mogelijke signalen. De organisatie heeft een voorziening voor het ontvangen van nieuwe ontwikkelingen op het gebied van ondermijningsrisico's.	Er zijn processen m.b.t. certificering, training en opleiding voor medewerkers en persoonlijke ontwikkelingsplannen worden gehanteerd. **Ondermijningspecifieke beheersmaatregel:** (Onderwerpspecifieke) beleidsregels en procedures zijn opgenomen in een jaarlijks bewustzijnsprogramma over ondermijning en de daarbij behorende actuele risico's.	Personeel en relevante belanghebbenden krijgen passende bewustwording, opleiding en training als ook regelmatige, relevante updates over het (onderwerpspecifieke) beleid en procedures m.b.t. m.b.t. informatiebeveiliging. **Ondermijningspecifieke beheersmaatregel:** Er wordt jaarlijks een specifieke bewustzijnstraining voor ondermijning gegeven t.b.v. vroegtijdige signalering van (actuele) ondermijningsactiviteiten. De organisatie meet de mate waarin personeel bewust is van de mogelijkheid om signalen te melden. In contacten met leveranciers wordt het onderwerp ondermijning periodiek en expliciet besproken.
NDO 2	**Meldpunt ondermijning** Wordt gebruik gemaakt van een ondermijningsmeldpunt?	De organisatie heeft een voorziening voor het melden van signalen die mogelijk wijzen op ondermijning. Medewerkers worden tijdens het onboardingsproces geïnformeerd over de voorziening.	Alle medewerkers worden periodiek bewust gemaakt dat zij signalen die mogelijk wijzen op ondermijning kunnen melden via de door de organisatie gekozen voorziening. Melders krijgen altijd (in meer of mindere mate) reactie op de melding die zij hebben gedaan.	De werking van de voorziening voor het melden van signalen die mogelijk wijzen op ondermijning wordt jaarlijks geëvalueerd en teruggekoppeld aan de medewerkers.
8.1	**'User endpoint devices'** Wordt gebruikersapparatuur (laptop, PC, tablet, smartphone) dat als onderdeel van de werkplek fungeert beschermd?	Er is geen formeel beleid wat gebruikers wel en niet mogen in het gebruik van (mobiele) informatiesystemen. Er vindt ad hoc registratie van systemen plaats en mogelijk maken medewerk(st)ers gebruik van privémiddelen voor zakelijke doeleinden zonder dat daar beleid voor is. **Ondermijningspecifieke beheersmaatregel:** De organisatie informeert medewerkers over de risico's van vermenging van privé-informatie met zakelijke informatie in het licht van ondermijning.	Verantwoordelijkheden m.b.t. systemen gebruikt door eindgebruikers zijn vastgelegd en in principe bekend bij eindgebruikers. Hier hoeft niet actief op te worden gecontroleerd. Er is bij de organisatie beleid en een methodiek die bepaalt welke systemen er welke toegang hebben tot informatie van de organisatie. Er is echter geen sprake van structureel (remote) beheer van deze systemen. **Ondermijningspecifieke beheersmaatregel:** De organisatie legt afspraken over het gebruik van privé en zakelijke accounts vast.	Gebruikers zijn zich bewust van procedures en vereisten in het gebruik van informatiesystemen, onder meer m.b.t. afsluiten wanneer niet in gebruik en handelen in openbare ruimtes. Er is (waar van toepassing) gecontroleerd beleid voor BYOD (Bring Your Own Device). De status van systemen (bijvoorbeeld m.b.t. patches en encryptie) wordt geregistreerd en installatie van software op werkplekken wordt door de organisatie beheerd. Er is sprake van een technische en organisatorische beheersing van alle door eindgebruikers gebruikte apparatuur. **Ondermijningspecifieke beheersmaatregel:** User end point devices zijn indien mogelijk gekoppeld aan persoonlijke accounts en zijn gekoppeld aan de dreigingsanalyse van Ondermijningspecifieke risico's
8.15	**Genereren, bewaren en beoordelen van logbestanden** Wordt er gebruik gemaakt van logbestanden?	Er vindt geen actief gebruik van logbestanden plaats. Wanneer logs worden gegenereerd, gebeurt dit meestal onbewust ('standaard instellingen') en er wordt zelden of nooit actief naar gekeken. **Ondermijningspecifieke beheersmaatregel:** De organisatie heeft waar mogelijk de standaardinstellingen voor het genereren van logs geactiveerd.	Er is beleid met betrekking tot welke activiteiten gelogd moeten worden. Toegang tot logbestanden is voorbehouden aan (systeem)beheerders. Toegang tot persoonsgegevens wordt (indien mogelijk) geregistreerd. **Ondermijningspecifieke beheersmaatregel:** Wijzigingen worden gelogd: – het aansluiten of verwijderen van devices; – de gelukte en mislukte inlogpogingen;	Logbestanden worden gericht gegenereerd en beschermd. Beoordeling vindt regelmatig plaats met als doel afwijkingen ten opzichte van normaal gebruik/functioneren te kunnen vaststellen en rapporteren. Logbestanden worden beschouwd als mogelijk bewijsmateriaal, waarbij toegang door beheerders en de integriteit van de bestanden wordt beheerst. Mogelijkheden tot manipulatie worden technisch voorkomen of gecompenseerd door organisatorische maatregelen. Geregistreerd wordt wie wanneer toegang had tot welke persoonsgegevens en welke aanpassingen er evt. zijn doorgevoerd. Er is een procedure om te bewerkstelligen dat persoonsgegevens in logbestanden wordt gewist of niet-identificeerbaar gemaakt, zoals gespecificeerd is in het bewaarschema. **Ondermijningspecifieke beheersmaatregel:** Loginstellingen worden jaarlijks getoetst op de detectie van insider threat

Met uitzondering van het exacte lettertype en kleurstelling wordt bovenstaand normkader tekstueel exact zo in de tool opgenomen waarmee zowel de organisatie als de auditoren werken met het NDO.