Informatiebeveiligingseisen

1. Inleiding

Verkoper en CWT zijn een overeenkomst aangegaan op grond waarvan Verkoper ermee heeft ingestemd diensten en/of producten te leveren op de voorwaarden in die overeenkomst (“Overeenkomst”). Verkoper stemt ermee in diensten en producten aan CWT te zullen leveren die voldoen aan de informatiebeveiligingseisen in dit document ("Informatiebeveiligingseisen") en de vereiste maatregelen voor informatiebeveiliging (“**Technische en Organisatorische Beveiligingsmaatregelen**”) en ervoor te zorgen dat de Derde Partijen die namens hem handelen hetzelfde doen. De Informatiebeveiligingseisen en Technische en Organisatorische Beveiligingsmaatregelen zijn opgenomen in en maken deel uit van deze overeenkomst.

2. Definities

2.1 Tenzij de gedefinieerde termen in deze voorwaarden anders zijn beschreven of uiteengezet, zullen ze dezelfde betekenis hebben als in de Overeenkomst. De navolgende gedefinieerde termen zullen van toepassing zijn op deze Informatiebeveiligingseisen. Als er sprake is van tegenstrijdigheid tussen de definitie in deze Overeenkomst en die in dat document, prevaleert de definitie uit dit document.

“**Partners**” wil zeggen - tenzij anders in de Overeenkomst aangegeven - met betrekking tot een partij, een bedrijf of andere rechtspersoon, op de datum van ondertekening van de Overeenkompst, direct of indirect: (i) die toezicht houdt op een partij; of (ii) waarop toezicht wordt gehouden door een partij; of (iii) waarop toezicht wordt gehouden door een bedrijf of entiteit die direct of indirect toezicht houdt op een partij. Voor deze doeleinden betekent "toezicht houden op" het recht om meer dan vijftig procent (50%) van de stemmen uit te brengen of een soortgelijk recht van eigendom; maar enkel voor de periode dat een dergelijk toezicht bestaat.

“Geautoriseerde Medewerker” wil zeggen medewerkers van Verkoper die kennis moeten nemen van of anderszins toegang hebben tot Vertrouwelijke en Persoonlijke Informatie om Verkoper in staat te stellen zijn verplichtingen op grond van deze Overeenkomst na te komen.

“**Geautoriseerde Partij” of “Geautoriseerde Partijen**” wil zeggen de (i) Geautoriseerde Medewerkers van Verkoper; en (ii) Derde Partijen (hieronder gedefinieerd) die kennis moeten nemen van of anderszins toegang hebben tot Vertrouwelijke en Persoonlijke Informatie om Verkoper in staat te stellen zijn verplichtingen op grond van deze Overeenkomst na te komen, en die schriftelijk gebonden zijn aan geheimhoudings- en andere verplichtingen die voldoende zijn om de Vertrouwelijke en Persoonlijke informatie te beschermen in overeenstemming met de algemene voorwaarden van de Overeenkomst en dit document.

"Vertrouwelijke Informatie" is alle commercieel gevoelige, eigendoms- of andere vertrouwelijke informatie betreffende (a) CWT; (b) een klant van CWT; (c) medewerkers van CWT en (d) CWT's onafhankelijke partners en joint venturers of (e) de inhoud en/of het doel van de Overeenkomst, of dit nu mondeling, schriftelijk of op een andere wijze direct of indirect in het bezit van de Verkoper of in het bezit van Geautoriseerde Partijen is gekomen, ten

gevolge van of in verband met deze Overeenkomst. Om elke twijfel weg te nemen, zullen alle werkproducten Vertrouwelijke Informatie bevatten.

"CWT" is - tenzij anders in de overeenkomst aangegeven - het in de Overeenkomst genoemde bedrijf CWT, alsmede zijn partners.

"**Gedemilitariseerde zone**" of "**DMZ**" is een netwerk of subnetwerk dat zich bevindt tussen een vertrouwd intern netwerk, zoals een zakelijk privé Local Area Network (LAN) en een niet-vertrouwd extern netwerk, zoals het openbaar internet. Een DMZ helpt te voorkomen dat gebruikers van buitenaf direct toegang verkrijgen tot interne systemen en andere bronnen.

"Procedure voor Incidentbeheer" is een door Verkoper ontwikkelde, gedocumenteerde methode en procedure die moet worden gevolgd in het geval van een actuele of vermoedelijke aanval op, onrechtmatige toegang tot, ongeautoriseerde toegang tot, verlies van of een andere inbreuk die betrekking heeft op de vertrouwelijkheid, beschikbaarheid of integriteit van de Vertrouwelijke en Persoonlijke informatie.

"Maskeren" is een proces waarbij informatie die op een scherm wordt weergegeven wordt verborgen.

"Mobiele en Draagbare Apparaten" zijn mobiele en/of draagbare computers, apparaten, media en systemen die eenvoudig kunnen worden gedragen, verplaatst of vervoerd en die conform de Overeenkomst worden gebruikt. Voorbeelden van dergelijke apparaten zijn laptops, tablets, USB-drives, USB-sticks, Persoonlijke Digitale Assistenten (PDA's), mobiele of datatelefoons of andere draadloze, rand- of verwijderbare apparatuur, of randapparatuur met het vermogen om Vertrouwelijke en Persoonlijke informatie op te slaan.

"Persoonlijke Informatie" is, tenzij anders aangegeven in de Overeenkomst, zoals gedefinieerd in de Richtlijn (EU) 2016/679 en andere toepasselijke wereldwijde informatiebeveiligings-, databeschermings- en privacywetten, is alle informatie met betrekking tot een geïdentificeerd of identificeerbaar natuurlijk persoon die, direct of indirect, kan worden geïdentificeerd, in het bijzonder aan de hand van een identificatienummer of een of meer factoren die specifiek zijn voor zijn of haar fysieke, fysiologische, mentale, economische, culturele of sociale identiteit. Persoonlijke Informatie is het eigendom van CWT, niet van Verkoper.

"Security Gateway" betekent een set van controlemechanismen tussen twee of meer netwerken met verschillende betrouwbaarheidsniveaus die passerend verkeer, en verkeer dat probeert te passeren, filteren en loggen, tussen netwerken, en de bijbehorende administratieve en beheerservers. Enkele voorbeelden van Security Gateways zijn firewalls, firewall beheerservers, hop boxen, session border controllers, proxyservers en apparaten die onrechtmatige toegang voorkomen.

"Krachtige Authenticatie" houdt het gebruik in van authenticatiemechanismen en -methoden die meerdere authenticatiefactoren vereisen, inclusief ten minste twee van de volgende: (1) kennis – iets dat de gebruiker weet, bv. een wachtwoord of een persoonlijk gegevensnummer,

en (2) eigendom – iets dat de gebruiker bezit, bv. een token, smart card, mobieltje, en (3) inherentie – iets dat de gebruiker is, bv. een vingerafdruk.

"Krachtige Encryptie" houdt het gebruik in van encryptietechnologieën met minimale sleutellengtes van 256 bits voor symmetrische encryptie en 1024 bits voor asymmetrische encryptie, waarvan de kracht een redelijke garantie biedt dat de versleutelde informatie zal worden beschermd tegen ongeautoriseerde toegang en in staat is om de vertrouwelijkheid en privacy van de versleutelde informatie te beschermen, en die een gedocumenteerd beleid omvat voor het beheer van encryptiesleutels en bijbehorende procedures die in staat zijn om de vertrouwelijkheid en privacy te beschermen van de sleutels en wachtwoorden die worden gebruikt voor toegang tot het encryptiealgoritme. Krachtige Encryptie is inclusief, maar niet beperkt tot: SSL v3.0+/TLS v1.0+, Point to Point Tunneling Protocol (PPTP), AES 256, FIPS 140-2 (alleen Amerikaanse overheid), RSA 1024 bit, SHA1/SHA2/SHA3, Internet Protocol Security (IPSEC), SFTP, SSH, Vormetric v4 of WPA2.

“Technische en Organisatorische Beveiligingsmaatregelen" betekent alle onder deze Informatiebeveiligingseisen vereiste activiteiten voor het verkrijgen van toegang tot, het beheren, overdragen, verwerken, opslaan, bewaren en vernietigen van informatie of gegevens; conform de overeenkomst en toepasselijke informatieprivacy- en databeschermingswetten de betrokken partijen bekend te maken en in kennis te stellen; en om informatie of gegevens te beschermen, teneinde beschikbaarheid, integriteit, vertrouwelijkheid en privacy te garanderen, of personen op de hoogte te stellen van het eventueel nalatig zijn in het beschermen van dergelijke informatie of gegevens. De maatregelen zijn inclusief, maar niet beperkt tot de maatregelen die vereist of geacht worden vereist te zijn op grond van de Algemene verordening gegevensbescherming (AVG) van de EU, de Richtlijn betalingsdiensten van de EU, de California Consumer Privacy Act, NYS DFS 23 NYCRR 500, de Amerikaanse Gramm-Leach Bliley Act (GLBA), de Amerikaanse Health Insurance Portability and Accountability Act (HIPAA), de vereisten voor gegevensprivacy van de EU en Zwitserland en andere internationale en Amerikaanse wetten, officiële wettelijke interpretaties of zaken die een precedent scheppen en die verband houden met informatie of gegevens onder de Overeenkomst.

"Derde Partij" betekent subcontractanten, adviseurs, tijdelijke medewerkers, contractanten of aanvullende verkopers van Verkoper en/of tussenpersonen die namens de Verkoper handelen, en is inclusief elke definitie van Derde Partij onder de Europese, Amerikaanse of andere internationale wetgeving.

"**Verkoper**" wil zeggen de in de Verklaring genoemde aanbestedende partij samen met zijn partners en Derde Partijen.

3. Organisatie van Informatiebeveiliging

Verkoper zal ten minste:

3.1 garanderen dat alleen Geautoriseerde Partijen toegang krijgen tot Vertrouwelijke en Persoonlijke Informatie;

3.2 technische en Organisatorische Beveiligingsmaatregelen invoeren die niet minder strikt zijn dan de beste praktijken op het gebied van informatiebeveiliging om de integriteit, beschikbaarheid en vertrouwelijkheid van Vertrouwelijke en Persoonlijke Informatie en andere niet-openbare informatie te beschermen en onbevoegd(e) toegang tot, verwerving, vrijgave, vernietiging, wijziging, accidenteel verlies of misbruik van of schade aan de Vertrouwelijke of Persoonlijke Informatie te voorkomen;

3.3 zorgdragen voor het instellen, implementeren en handhaven van een geschikt beleid en een programma met organisatorische, operationele, administratieve, fysieke en Technische en Organisatorische Beveiligingsmaatregelen, consistent met de beste praktijken in de branche, geschikt om (1) elke toegang door niet-Geautoriseerde Partijen tot de Vertrouwelijke en Persoonlijke Informatie te voorkomen die niet is toegestaan volgens de Overeenkomst of deze Informatiebeveiligingseisen, en (2) om alle toepasselijke wet- en regelgeving en normen van de sector na te leven en hieraan tegemoet te komen;

3.4 geautoriseerde Partijen die toegang hebben tot Vertrouwelijke en Persoonlijke Informatie supervisie, begeleiding en training bieden op het gebied van de Technische en Organisatorische Beveiligingsmaatregelen. Verkoper zal ook een training op het gebied van Technische en Organisatorische Beveiligingsmaatregelen geven bij het in dienst nemen van een Geautoriseerde Medewerker en voordat een Geautoriseerde Partij toegang krijgt tot Vertrouwelijke en Persoonlijke Informatie. Er zal ten minste jaarlijks en zo snel mogelijk na een belangrijke wijziging in de Technische en Organisatorische Beveiligingsmaatregelen van Verkoper een opfristraining worden gegeven;

3.5 Geautoriseerde Partijen met aanzienlijke beveiligingsverplichtingen, inclusief, maar niet beperkt tot, functies op het gebied van human resources en informatietechnologie, en alle technische administratorfuncties, een gespecialiseerde training geven. De speciale training zal op zijn minst bestaan uit, voor zover van toepassing op de functie: informatiebeveiligingsprocedures, aanvaardbaar gebruik van informatiebeveiligingsbronnen, huidige bedreigingen van informatiesystemen, beveiligingsmogelijkheden van specifieke systemen en veilige toegangsprocedures;

3.6 de benodigde stappen nemen ter voorkoming van ongeautoriseerde toegang tot of verlies van de Vertrouwelijke en Persoonlijke Informatie en de diensten, systemen, apparaten of media die deze informatie bevatten;

3.7 gebruikmaken van risicoanalysemethoden en -procedures om regelmatig systemen te beoordelen die worden gebruikt om diensten of producten aan CWT te leveren. Verkoper zal ook dergelijke risico's zo snel als redelijkerwijs mogelijk verhelpen en ervoor zorgen dat het hoofd kan worden geboden aan het risiconiveau voor de Vertrouwelijke en Persoonlijke Informatie gezien de bedreigingen op het moment van identificatie. Een procedure in werking stellen om het mogelijk te maken risico's of verdachte incidenten aan het beveiligingsteam van Verkoper te rapporteren;

3.8 voor zover de Verkoper diensten in navolging van de Overeenkomst verleent in de faciliteiten van CWT of diensten, systemen, apparaten of media gebruikt die in het bezit zijn van of worden gebruikt of beheerd door CWT, ervoor zorgen dat alle Geautoriseerde Partijen het aan Verkoper ter beschikking gestelde beleid van CWT dat van toepassing is op een zodanige toegang, op zijn verzoek, naleven. Verkoper zal CWT per ommegaande schriftelijk op de hoogte brengen wanneer een Geautoriseerde Partij geen toegang meer nodig heeft tot Vertrouwelijke of Persoonlijke Informatie zodat de Verkoper producten of diensten aan CWT kan leveren, waaronder, zonder beperking, wanneer het dienstverband met een Geautoriseerde Partij wordt beëindigd of de Geautoriseerde Partij niet langer diensten verleent op grond van de Overeenkomst;

3.9 bijhouden welke Geautoriseerde Partijen en bronnen van Verkoper Vertrouwelijke toegang krijgen tot Persoonlijke Informatie en het overdragen, geheimhouden, opslaan of gebruiken;

3.10 op alle Geautoriseerde Partijen voorafgaand aan indienstneming, in de mate die bij wet wordt toegelaten, uitvoerige achtergrondcontroles uitvoeren. Bij deze uitvoerige achtergrondcontroles op personen worden, op zijn minst, eerdere dienstverbanden van de persoon, strafblad, kredietgeschiedenis, referenties, en andere controles die in de branche gangbaar zijn nagetrokken;

3.11 één of meer gekwalificeerde personeelsleden aanwijzen die worden belast met de handhaving van het informatiebeveiligingsprogramma. Verkoper zorgt ervoor dat zijn beveiligingspersoneel een redelijk en noodzakelijk niveau van ervaring en opleiding op het gebied van informatiebeveiliging heeft. Op verzoek zal Verkoper CWT een contactpunt bieden voor alle kwesties met betrekking tot informatiebeveiliging.

3.12 van Geautoriseerde Partijen eisen dat zij zich contractueel verbinden aan geheimhoudings- of vertrouwelijkheidsverplichtingen voordat zij toegang krijgen tot Vertrouwelijke en Persoonlijke Informatie;

3.13 ervoor zorgen dat alle Geautoriseerde Partijen die werkzaamheden uitvoeren op grond van de Overeenkomst of mogelijk toegang krijgen tot Vertrouwelijke of Persoonlijke Informatie deze Technische en Organisatorische Veiligheidsmaatregelen naleven en gehouden zijn aan een schriftelijke overeenkomst die niet minder beperkend is dan deze Informatiebeveiligingseisen.

4. <u>Fysieke Beveiliging en Beveiliging van de Omgeving</u>

Verkoper zal ten minste:

4.1 ervoor zorgen dat alle systemen van Verkoper en andere bronnen bedoeld voor gebruik door meerdere gebruikers zich in veilige fysieke faciliteiten bevinden met beperkte toegang voor alleen geautoriseerde personen;

4.2 voor auditdoeleinden, de toegang tot de fysieke faciliteiten controleren en registreren waar zich systemen en andere bronnen bedoeld voor gebruik door meerdere gebruikers bevinden,

die worden gebruikt in verband met de uitvoering van de Verkoper van zijn verplichtingen onder de Overeenkomst;

4.3 vereisen dat alle Geautoriseerde Partijen zich houden aan een 'opgeruimd bureau'-beleid en de schermen van hun werkstations sluiten alvorens hun werkplekken te verlaten;

4.4 bij beëindiging van de werkzaamheden of het contract alle bedrijfsmiddelen in ontvangst nemen;

4.5 de fysieke toegang tot zijn faciliteiten beperken en monitoren in overeenstemming met de volgende vereisten:

a. Toegang van bezoekers wordt gelogd en de log wordt gedurende drie (3) maanden bewaard en bevat de naam van de bezoeker, het bedrijf dat hij/zij vertegenwoordigt en de naam van de medewerker die toestemming geeft voor de fysieke toegang. Bezoekers moeten te allen tijde door een medewerker van de Verkoper worden begeleid.
b. De toegang is beperkt tot bevoegde medewerkers, op basis van 'need to know'.
c. Alle medewerkers dienen een door het bedrijf verstrekte naambadge te dragen en alle bezoekers of Derde Partijen dienen een door het bedrijf verstrekte gastenbadge te dragen.
d. Bij beëindiging van de werkzaamheden van het personeelslid of de Derde partij wordt onmiddellijk de toegang ontzegd en dienen alle middelen voor fysieke toegang, zoals sleutels, toegangskaarten, etc. geretourneerd te worden of onbruikbaar te worden gemaakt
e. Het datacentrum of de computerruimte is afgesloten en de toegang is beperkt tot degenen die toegang nodig hebben om hun functie uit te voeren.
f. Waar wettelijk toegestaan videocamera's gebruiken om individuele fysieke toegang tot kwetsbare ruimtes te monitoren; en deze beelden regelmatig beoordelen. Videobeelden moeten gedurende minimaal drie (3) maanden worden bewaard.
g. Apparatuur die wordt gebruikt om Vertrouwelijke en Persoonlijke Informatie op te slaan, te verwerken of over te brengen, dient fysiek te worden beveiligd, met onder meer draadloze toegangspunten, gateways, handapparaten, netwerk-/communicatiehardware en telecommunicatielijnen;

4.6 controles implementeren ter minimalisering van het risico van en ter bescherming tegen fysieke bedreigingen;

4.7 ervoor zorgen dat alle hardware-activa met Vertrouwelijke en Persoonlijke Informatie wordt gebruikt en gehanteerd in overeenstemming met de door de fabrikant aanbevolen servicevereisten;

4.8 vergaderruimtes en andere openbaar toegankelijke netwerken en netwerkjacks logisch en fysiek van het interne netwerk van Verkoper scheiden en beperken tot alleen geverifieerde gebruikers of standaard uitschakelen;

4.9 alle apparaten die betaalkaartgegevens opslaan door middel van directe fysieke interactie beschermen tegen sabotage en vervanging door periodiek de oppervlakken van apparaten te

inspecteren om sabotage of vervanging te detecteren; en medewerkers een training bieden zodat ze zich bewust zijn van pogingen tot sabotage of vervanging van apparaten;

4.10 toegangspunten als leverings- en laadruimtes en de toegangspunten van alle centra die Vertrouwelijke en Persoonlijke Informatie gebruiken, beheren, opslaan of verwerken, controleren en van elkaar scheiden;

4.11 ervoor zorgen dat de eigen datacentra van de Verkoper beschikken over apparatuur voor verwarming, koeling, vuuronderdrukking en detectie van water, warmte en rook. In deze datacentra en computerruimtes mag zich geen brandbaar materiaal (bv., dozen, papier, enz.) bevinden of dit materiaal moet opgeslagen zijn in metalen kasten.

5. Toegangscontrole

Verkoper zal ten minste:

5.1 alle benodigde stappen nemen om te voorkomen dat iemand die geen Geautoriseerde Partij is, toegang krijgt tot de Vertrouwelijke en Persoonlijke Informatie op een wijze of met een reden die niet wordt geautoriseerd door CWT en de Overeenkomst.

5.2 de informatie van CWT scheiden van de gegevens van de andere klanten van Verkoper of de applicaties en informatie van Verkoper zelf, door gebruik te maken van andere fysieke servers of door logische toegangscontroles te gebruiken in het geval er geen sprake is van fysieke scheiding van servers;

5.3 de juiste eigenaren identificeren en vragen om toegang tot systemen die worden gebruikt voor toegang tot en gebruik, beheer en opslag van de Vertrouwelijke en Persoonlijke Informatie ten minste elk kwartaal te beoordelen en goed te keuren om niet-geautoriseerde toegang te voorkomen; en zal goedkeuringen van toegang handhaven en bijhouden;

5.4 binnen 24 uur de toegang tot systemen met Vertrouwelijke en Persoonlijke Informatie beëindigen voor een Geautoriseerde partij die de relatie met Verkoper beëindigt; en redelijke procedures onderhouden om binnen drie werkdagen de toegang op te heffen tot dergelijke systemen als deze niet langer nodig of relevant is voor het uitvoeren van hun taken. Alle andere gebruikers-ID's moeten na 90 kalenderdagen inactiviteit onbruikbaar worden gemaakt of worden verwijderd;

5.5 de toegang van systeembeheerders (ook bekend als root, privileged en superuser) tot besturingssystemen bedoeld voor gebruik door meerdere gebruikers beperken tot personen die een toegang van een dergelijk hoog niveau nodig hebben voor de uitoefening van hun werkzaamheden. Gebruikmaken van uitcheck-ID’s voor systeembeheerders met individuele inloggegevens voor gebruikers en activiteitenlogs om toegang met een hoog beveiligingsniveau te handhaven en toegang met een hoog niveau te beperken tot een zeer beperkt aantal gebruikers; applicatie-, database-, netwerk- en systeembeheerders vragen om de toegang van gebruikers te beperken tot enkel commando's, data, systemen en andere bronnen die ze nodig hebben voor het uitvoeren van geautoriseerde werkzaamheden.

Systeembeheerdersrollen en toegangslijsten moeten ten minste eens per jaar worden gecontroleerd;

5.6 de regel van minimale privileges toepassen (ofwel de toegang beperken tot de opdrachten, informatie, systemen en andere middelen die nodig zijn om de geautoriseerde taken van een functie uit te voeren);

5.7 krachtige Authenticatie behoeven voor de toegang van beheerders die niet via consoles verloopt en toegang op afstand en voor alle toegang van beheerders tot cloud-omgevingen;

5.8 een verbod uitvaardigen en gebruikmaken van toepasselijke Technische en Organisatorische Veiligheidsmaatregelen, om ervoor te zorgen dat Vertrouwelijke en Persoonlijke Informatie niet kan worden gekopieerd, verplaatst of bewaard op lokale hard drives of Vertrouwelijke en Persoonlijke Informatie knippen en plakken of printen;

5.9 mogelijkheden voor gebruik of toegang op afstand alleen activeren wanneer nodig, monitoren wanneer in gebruik en onmiddellijk deactiveren na gebruik;

5.10 Sterke authenticatie vragen om verbinding te kunnen maken met interne hulpbronnen van Verkoper die Vertrouwelijke en Persoonlijke Informatie bevatten.

6. Identificatie en Authenticatie

Verkoper zal ten minste:

6.1 unieke gebruikers-ID's toewijzen aan individuele gebruikers en authenticatiemechanismen toewijzen aan elk individueel account;

6.2 gebruikmaken van een gedocumenteerde beheerproces voor de levenscyclus van een gebruikers-ID inclusief, maar niet beperkt tot, procedures voor goedgekeurde accountcreatie, tijdige accountverwijdering en accountwijziging (bijv. wijzigingen van privileges, toegangsperiode, functies/taken) voor alle toegang tot Vertrouwelijke en Persoonlijke Informatie en in alle omgevingen (bijv. productie, test, ontwikkeling, etc.). Dit proces zal inclusief ten minste een keer per kwartaal een herziening van toegangsprivileges en geldigheid van accounts zijn;

6.3 alle toegang tot Vertrouwelijke en Persoonlijke Informatie beperken met gebruikmaking van een geldig gebruikers-ID en wachtwoord, en vereisen dat voor unieke gebruikers-ID's het volgende wordt aangewend: een wachtwoord of wachtwoordzin, tweeledige authenticatie of een biometrische waarde;

6.4 wachtwoordcomplexiteit vereisen en voldoen aan de volgende voorwaarden ten aanzien van de samenstelling van het wachtwoord: een minimum van acht (8) karakters lang voor systeemwachtwoorden en vier (4) karakters voor toegangscodes voor tablets en smartphones. Systeemwachtwoorden moeten drie (3) van de volgende elementen bevatten: hoofdletters, kleine letters, getallen of speciale karakters. Wachtwoorden dienen ook niet

hetzelfde te zijn als het gebruikers-ID waaraan ze zijn gekoppeld, een woordenboekwoord, opeenvolgende of herhalende cijfers te bevatten, of hetzelfde te zijn als één van de laatste vijf wachtwoorden. Vereisen dat wachtwoorden regelmatig verlopen, uiterlijk na negentig (90) dagen. Alle wachtwoorden maskeren als deze worden getoond;

6.5 mislukte inlogpogingen beperken tot maximaal vijf (5) inlogpogingen binnen 24 uur en het gebruikersaccount sluiten als deze limiet herhaaldelijk wordt bereikt. De toegang tot het gebruikersaccount kan vervolgens weer gereactiveerd worden door middel van een handmatig proces waarbij verificatie van de identiteit van de gebruiker is vereist;

6.6 de identiteit van de gebruiker verifiëren, eenmalig gebruik instellen en wachtwoorden opnieuw instellen met een unieke waarde voor elke gebruiker. Na het eerste gebruik systematisch een onmiddellijke wijziging bewerkstelligen;

6.7 gebruikmaken van een veilige methode voor de overdracht van authenticatiereferenties (bijv. wachtwoorden) en authenticatiemechanismen (bijv. tokens of smartcards).;

6.8 service account en proxy wachtwoorden beperken tot een minimum van 12 karakters, inclusief hoofdletters, kleine letters en numerieke karakters, alsmede speciale symbolen. service account en proxy wachtwoorden ten minste 1 keer per jaar wijzigen en na beëindiging van het dienstverband van iemand die het wachtwoord kent;

6.9 interactieve sessies beëindigen, of een veilige, vergrendelende screensaver activeren die authenticatie vereist, na een periode van inactiviteit van maximaal vijftien (15) minuten;

6.10 een authenticatiemethode gebruiken die afhankelijk is van de gevoeligheid van de Vertrouwelijke en Persoonlijke Informatie. Telkens als authenticatiegegevens worden opgeslagen, deze met gebruikmaking van Krachtige Encryptie beschermen;

6.11 systemen zodanig configureren dat ze na een maximale periode van inactiviteit uitschakelen, en wel als volgt: (server 15 minuten), werkstation (15 minuten), mobiel apparaat (4 uur), Dynamic Host Configuration Protocol (7 dagen), Virtueel Privénetwerk (24 uur).

7. <u>Informatiesystemen Acquisitie, Ontwikkeling en Onderhoud</u>

Verkoper zal ten minste:

7.1 een waarschuwingsbanner op de inlogschermen of –pagina's plaatsen, zoals schriftelijk gespecificeerd door CWT, voor merkproducten of -diensten van CWT of voor producten en software die is ontwikkeld voor CWT;

7.2 alle toegangsapparaten die eigendom zijn van of verstrekt zijn door CWT zo snel als haalbaar is retourneren, maar in geen geval later dan vijftien (15) dagen na het snelste van het volgende:

a. verlopen of beëindiging van de Overeenkomst;

b. het verzoek van CWT om dit eigendom te retourneren; of
c. de datum waarop Verkoper deze apparaten niet meer nodig heeft;

7.3 een doeltreffende applicatiemanagement-methode gebruiken die technische en organisatorische veiligheidsmaatregelen voor informatie in het softwareontwikkelingsproces integreert, en ervoor zorgen dat technische en organisatorische veiligheidsmaatregelen voor informatie op basis van de best practices van de industrie tijdig door Verkoper worden geïmplementeerd;

7.4 in de branche standaard ontwikkelingsprocedures volgen, inclusief scheiding van toegang en code tussen niet-productie- en productieomgevingen en samengaande scheiding van verplichtingen tussen dergelijke omgevingen;

7.5 ervoor zorgen dat er regelmatig interne informatiebeveiligingscontroles voor softwareontwikkeling plaatsvinden en de best practices van de sector weerspiegelen, en deze controles tijdig herzien en implementeren;

7.6 de veiligheid van het ontwikkelingsproces beheren en ervoor zorgen dat veilige coderingspraktijken worden geïmplementeerd en gevolgd, inclusief toepasselijke cryptografische controles, beschermingen tegen kwaadaardige code, en een peerreview-proces;

7.7 ten minste jaarlijks en na alle belangrijke wijzigingen aan broncodes of configuraties die in lijn zijn met OWASP, CERT, SANS Top 25 en PCI-DSS gebruiken een penetratietest uitvoeren op functioneel complete applicaties, alvorens ze vrijgegeven worden voor productie en daarna. Alle exploitabele kwetsbaarheden verhelpen vóór het inzetten in de productieomgeving;

7.8 geanonimiseerde of gecodeerde gegevens gebruiken in niet-productieomgevingen. nooit productiegegevens als platte tekst gebruiken in een niet-productieomgeving, en nooit Vertrouwelijke en Persoonlijke Informatie gebruiken in niet-productieomgevingen, om welke reden dan ook. Ervoor zorgen dat alle testgegevens en -accounts zijn verwijderd vóór de productrelease;

7.9 open of gratis broncode die is goedgekeurd door CWT, software, toepassingen of diensten controleren op tekortkomingen, bugs, beveiligingsproblemen of niet-naleving van de licentievoorwaarden voor open of gratis broncode. Verkoper zal CWT van tevoren op de hoogte brengen als hij open of gratis broncode gaat gebruiken en, als dit gebruik wordt goedgekeurd door CWT, CWT de naam, versie en URL van de open of gratis broncode verschaffen. Verkoper verklaart en garandeert dat (a) alle open of gratis broncode die hij gebruikt in zijn producten of diensten is gelicentieerd op grond van "permissieve" licenties inzake open of gratis code en niet op grond van beperkte, wederkerige, hereditaire of Copyleft-licenties; (b) Verkoper het recht heeft de open of gratis broncode vrijelijk te wijzigen en aan te passen en de open of gratis broncode te combineren of open of gratis broncode op te nemen in gepatenteerde code zonder dat er beperkingen worden verbonden aan dergelijke wijzigingen, aanpassingen of combinaties of gepatenteerde code die open of gratis broncode bevat en de manier waarop deze daarna kunnen worden gelicentieerd (samen “afgeleide

werken") en (c) dat op dergelijke afgeleide werken geen licentie inzake open of gratis broncode van toepassing is waarin wordt geëist dat afgeleide werken worden gelicentieerd of kosteloos ter beschikking worden gesteld aan derden op grond van de voorwaarden van de licentie inzake open of gratis broncode;

7.10 onder de Overeenkomst gecreëerde code niet delen, ongeacht de ontwikkelingsfase, in een gedeelde omgeving of een omgeving die niet privé is, zoals een open toegangscode-bewaarplaats, ongeacht wachtwoordbescherming.

8. Software- en gegevensintegriteit

Verkoper zal ten minste:

8.1 in omgevingen waar antivirussoftware in de handel verkrijgbaar is, actuele anti-virussoftware geïnstalleerd hebben die draait en virussen en andere malware van alle systemen en apparaten scant en onmiddellijk verwijdert of in quarantaine plaatst;

8.2 niet-productie-informatie en -bronnen scheiden van productie-informatie en -bronnen;

8.3 ervoor zorgen dat teams een gedocumenteerde veranderingsbeheerproces gebruiken voor alle systeemwijzigingen, inclusief back-outprocedures voor alle productieomgevingen en noodwijzigingsprocessen. Testen, documentatie en goedkeuringen voor alle systeemwijzigingen opnemen en managementtoestemming vereisen voor belangrijke wijzigingen in dergelijke processen;

8.4 een PCI-zone ontwikkelen en onderhouden als de Verkoper gegevens van kaarthouders verwerkt of opslaat;

8.5 voor applicaties die een database gebruiken die wijzigingen aan de Vertrouwelijke en Persoonlijke Informatie toestaat, auditlogging-functies voor databasetransacties in werking stellen en bijhouden en auditlogs van databasetransacties gedurende minimaal een (1) jaar bewaren en drie (3) maanden onmiddellijk beschikbaar hebben voor analyse;

8.6 software beoordelen om veiligheidskwetsbaarheden gedurende de initiële implementatie en na belangrijke wijzigingen en updates te vinden en te verhelpen;

8.7 een kwaliteitsgarantietest uitvoeren voor de veiligheidscomponenten (bijv. testen van identificatie-, authenticatie- en autorisatiefuncties), alsmede elke andere activiteit die is ontwikkeld om de veiligheidsarchitectuur te valideren, gedurende de initiële implementatie en na belangrijke wijzigingen en updates.

9. Systeembeveiliging

Verkoper zal ten minste:

9.1 regelmatig de recentste versies van gegevensstroom- en systeemdiagrammen creëren en updaten die worden gebruikt voor toegang tot en gebruik, beheer en opslag van de Vertrouwelijke en Persoonlijke Informatie;

9.2 actief bronnen binnen de sector (bijv., www.cert.org en relevante mailinglijsten en websites van softwareverkopers) monitoren, voor tijdige notificatie van alle toepasselijke veiligheidswaarschuwingen betrekking hebbend op de systemen van Verkoper en andere informatiebronnen;

9.3 doeltreffend cryptografische sleutels beheren door toegang tot sleutels te verlagen tot het kleinste aantal benodigde beheerders, geheime en privé-cryptografische sleutels opslaan door te versleutelen met een sleutel die ten minste net zo sterk is als de sleutel voor gegevensencryptie, en deze afzonderlijk van de sleutel voor gegevensencryptie op te slaan in een veilig cryptografisch apparaat, op zo min mogelijk locaties. De standaardwaarde van de cryptografische sleutels bij de installatie wijzigen en ten minste elke twee jaar, en oude sleutels op veilige wijze wegdoen;

9.4 extern gerichte en interne systemen en andere informatiebronnen scannen, inclusief, maar niet beperkt tot, netwerken, servers en applicaties en databases, met toepasselijke, in de sector gangbare software voor het scannen op beveiligingskwetsbaarheden, ten minste elk kwartaal, en voorafgaand aan de release van applicaties en belangrijke wijzigingen en upgrades binnen tijdsbestekken voortvloeiend uit risicoanalyses die zijn gebaseerd op een IT-beleid en normen die redelijk en algemeen aanvaard zijn;

9.5 ervoor zorgen dat alle systemen en andere bronnen van Verkoper 'ondoordringbaar' zijn en blijven, inclusief, maar niet beperkt tot, het verwijderen of onbruikbaar maken van ongebruikte netwerken en andere diensten en producten (bijv. finger, rlogin, ftop en eenvoudige Transmission Control Protocol/Internet Protocol (TCP/IP) diensten en producten) en een systeemfirewall, Transmission Control Protocol (TCP) wrappers of gelijksoortige technologie installeren;

9.6 een of meer Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) of Intrusion Detection and Prevention Systems (IDP) met een actieve functioneringsmodus inzetten, die al het inkomende en uitgaande verkeer van systemen en andere bronnen in combinatie met de Overeenkomst monitoren, in omgevingen waarin een dergelijke technologie in de handel verkrijgbaar is en voor zover mogelijk;

9.7 een gedocumenteerd risicowaarderingsproces onderhouden overeenkomstig de best practices in de branche om beveiligingskwetsbaarheden in systemen of andere bronnen te beoordelen en verhelpen, inclusief, maar niet beperkt tot die door publicaties binnen de sector, het scannen op kwetsbaarheden, het scannen op virussen en het bestuderen van beveiligingslogs worden ontdekt, en onmiddellijk geschikte veiligheidspatches toepassen, gezien de mogelijkheid dat een dergelijke kwetsbaarheid kan worden of reeds wordt geëxploiteerd. Kritieke bevindingen van beveiligingskwetsbaarheden en patches moeten onmiddellijk bij de beschikbaarheid worden geïnstalleerd en in geen geval langer dan zeven (7) dagen na de release. Bevindingen met betrekking tot ernstige beveiligingskwetsbaarheden

en patches moeten binnen 30 dagen na de release worden geïnstalleerd. Bevindingen met betrekking tot gemiddeld ernstige beveiligingskwetsbaarheden en patches moeten binnen 90 dagen worden geïnstalleerd;

9.8 ten minste elk jaar en na elke belangrijke upgrade of wijziging van de infrastructuur of een applicatie intern en extern een algemene penetratietest uitvoeren;

9.9 ongeautoriseerde software die is ontdekt op de systemen van de Verkoper verwijderen of onbruikbaar maken en voor de branche standaard malwarecontroles uitvoeren, inclusief de installatie, regelmatige update en routinegebruik van antimalwareproducten voor alle diensten, systemen en apparaten die gebruikt kunnen zijn voor toegang tot de Vertrouwelijke en Persoonlijke Informatie. Waar dit haalbaar is betrouwbare en door de sector algemeen geaccepteerde antivirussoftware gebruiken en ervoor zorgen dat dergelijke virusdefinities up-to-date blijven;

9.10 redelijkerwijs up-to-date software gebruiken voor alle diensten, systemen en apparaten die kunnen worden gebruikt voor toegang tot Vertrouwelijke en Persoonlijke Informatie, inclusief een geschikt onderhouds- of besturingssysteem of -systemen en succesvolle installatie van redelijkerwijs up-to-date veiligheidspatches;

9.11 verantwoordelijkheden met betrekking tot veiligheidsbeheer voor het configureren van gastheer-besturingssystemen toekennen aan specifieke personen;

9.12 alle standaardaccountnamen en/of standaardwachtwoorden wijzigen.

10. Monitoring

Verkoper zal ten minste:

10.1 loggegevens voor Vertrouwelijke en Persoonlijke Informatie gedurende ten minste 12 maanden vanaf de datum dat de loggegevens zijn aangemaakt bewaren en zulke informatie binnen een redelijk tijdsbestek en op verzoek beschikbaar stellen aan CWT, tenzij anders aangegeven in deze Overeenkomst. Logboeken worden ontworpen om incidenten te detecteren en erop te reageren en bevatten onder meer, maar niet alleen, de volgende informatie:

a. alle toegang van individuele gebruikers tot Vertrouwelijke en Persoonlijke Informatie
b. alle acties die zijn genomen door personen met beheerders- of root-machtigingen
c. alle toegang van gebruikers tot audit-sporen
d. ongeldige logische toegangspogingen
e. gebruik van en veranderingen in de mechanismen voor identificatie en authenticatie;

10.2 de primaire systeemactiviteiten van de Derde Partijen van Verkoper registreren voor systemen die Vertrouwelijke en Persoonlijke Informatie bevatten;

10.3 de toegang tot beveiligingslogs beperken tot geautoriseerde personen, en beveiligingslogs beschermen tegen ongeautoriseerde wijziging;

10.4 een mechanisme implementeren dat wijzigingen detecteert (bijv. monitoren van bestandsintegriteit) om medewerkers te attenderen op ongeautoriseerde wijziging van kritische systeembestanden, configuratiebestanden of inhoudsbestanden; software configureren om wekelijks vergelijkingen van kritische bestanden te maken;

10.5 alle beveiligings- en beveiligingsgerelateerde auditlogs van systemen met Vertrouwelijke en Persoonlijke Informatie ten minste een keer per week controleren op afwijkingen en alle gelogde beveiligingsproblemen tijdig documenteren en verhelpen;

10.6 dagelijks alle veiligheidskwesties, -logs of systeemcomponenten die kaarthoudergegevens, logs of kritische systeemcomponenten opslaan, verwerken of overdragen beoordelen, en logs van servers en systeemcomponenten die veiligheidstaken verrichten.

11. Security Gateways

Verkoper zal ten minste:

11.1 Krachtige Authenticatie vereisen voor toegang voor administratieve en/of beheerdoeleinden tot Security Gateways, inclusief, maar niet beperkt tot, toegang met als doel het beoordelen van logbestanden;

11.2 gedocumenteerde controles, gedragsregels, processen en procedures hebben en gebruiken om ervoor te zorgen dat ongeautoriseerde gebruikers geen toegang tot Security Gateways hebben voor administratieve en/of beheerdoeleinden, en dat gebruikersautorisatieniveaus voor het administreren en beheren van Security Gateways toepasselijk zijn;

11.3 ten minste elke zes (6) maanden ervoor zorgen dat configuraties van Security Gateways ondoordringbaar zijn, door een steekproef te nemen bij de Security Gateways en te verifiëren dat elke standaardregelset en set met configuratieparameters het volgende waarborgt:

a. Internet Protocol (IP) source routing is uitgeschakeld;
b. het loopbackadres is verhinderd het interne netwerk binnen te gaan;
c. er zijn antispoofing-filters geïmplementeerd;
d. het is broadcast-pakketten niet toegestaan het netwerk binnen te gaan; e.
e. Internet Controle Message Protocol (ICMP) doorverwijzingen zijn uitgeschakeld;
f. alle regelsets eindigen met de vermelding "ALLEMAAL WEIGEREN", en
g. elke regel is traceerbaar voor een specifiek zakelijk verzoek;

11.4 ervoor zorgen dat monitoringtools worden gebruikt om te bevestigen dat alle aspecten van Security Gateways (bijv. hardware, firmware en software) continu operationeel zijn;

ervoor zorgen dat alle Security Gateways zodanig zijn geconfigureerd en geïmplementeerd dat alle niet-operationele Security Gateways elke toegang zullen weigeren;

11.5 ervoor zorgen dat inkomende pakketten van niet-vertrouwde externe netwerken moeten eindigen binnen de gedemilitariseerde zone ("DMZ") en niet de mogelijkheid hebben om direct door het vertrouwde interne netwerk te gaan. Alle inkomende pakketten die door het vertrouwde interne netwerk gaan, moeten allemaal voortkomen uit de DMZ. De DMZ moet van het niet-vertrouwde externe netwerk worden afgescheiden door gebruikmaking van een Security Gateway en van het vertrouwde interne netwerk worden afgescheiden door het gebruik van:

a. een andere Security Gateway, of
b. dezelfde Security Gateway die wordt gebruikt om de DMZ af te scheiden van het niet-vertrouwde externe netwerk, in welk geval de Security Gateway moet garanderen dat pakketten die worden ontvangen van het niet-vertrouwde externe netwerk onmiddellijk worden verwijderd of als ze niet worden verwijderd alleen naar de DMZ worden geleid als het enige wat met dergelijke inkomende pakketten gebeurt is dat ze eventueel in een log worden vermeld.

Het volgende moet zich alleen binnen het vertrouwde interne netwerk bevinden:

a. alle Persoonlijke Informatie of Vertrouwelijke bedrijfsgegevens van CWT die zijn opgeslagen zonder het gebruik van Krachtige Encryptie;
b. het officiële gegevensbestand met informatie;
c. databaseservers;
d. alle uitgevoerde logs, en
e. alle omgevingen die worden gebruikt voor ontwikkelen, testen, sandbox, productie en soortgelijke omgevingen; en alle broncodeversies;

11.6 authenticatiegegevens die niet worden beschermd door het gebruik van Krachtige Encryptie niet in de DMZ plaatsen.

12. Netwerkbeveiliging

Verkoper zal ten minste:

12.1 op verzoek van CWT een logisch netwerkdiagram aan CWT verstrekken, met gegevens over systemen en verbindingen met andere bronnen, waaronder routers, switches, firewalls, IDS-systemen, netwerktopologie, externe verbindingspunten, gateways, draadloze netwerken, en alle andere apparaten die CWT ondersteunen;

12.2 een formeel proces hanteren voor het goedkeuren, testen en documenteren van alle netwerkverbindingen en wijzigingen aan de firewall- en routerconfiguraties. Firewalls configureren om verdachte pakketten te weigeren en loggen, en alleen toepasselijk en geautoriseerd verkeer toe te staan, waarbij al het andere verkeer door de firewall wordt geweigerd. De firewall-regels elke zes maanden herzien;

12.3 een firewall installeren voor elke internetverbinding en tussen elke DMZ en de interne netwerkzone. Elk systeem met Vertrouwelijke en Persoonlijke Informatie moet zich in een

interne netwerkzone bevinden, afgezonderd van de DMZ en andere niet-vertrouwde netwerken;

12.4 indien nodig de firewall bij de buitengrens en intern monitoren om de stroom netwerkverkeer die de grens binnenkomt of verlaat te controleren en te beschermen;

12.5 een gedocumenteerd proces en gedocumenteerde controles bijhouden om ongeautoriseerde pogingen om toegang te verkrijgen tot de Vertrouwelijke en Persoonlijke Informatie te ontdekken en af te handelen;

12.6 wanneer internetgebaseerde diensten en producten aan CWT worden geboden, Vertrouwelijke en Persoonlijke Informatie beschermen door de implementatie van een netwerk DMZ. Webservers die diensten aan CWT bieden, zullen zich in de DMZ bevinden. Elk systeem en elke informatiebron die Vertrouwelijke en Persoonlijke Informatie opslaat (zoals applicatie- en databaseservers) zal zich in een vertrouwd intern netwerk bevinden. (Internetdiensten en -producten maken gebruik van DMZ);

12.7 ongeautoriseerd uitgaand verkeer beperken in het gebruik van applicaties die Vertrouwelijke en Persoonlijke Informatie verwerken, opslaan of overbrengen naar IP-adressen binnen de DMZ en het internet;

12.8 wanneer gebruik wordt gemaakt van draadloze netwerktechnologieën die zijn gebaseerd op radiofrequentie (RF) om ondersteuningsdiensten en producten aan CWT te leveren, ervoor zorgen dat alle overgebrachte Vertrouwelijke en Persoonlijke Informatie wordt beschermd door het gebruik van krachtige encryptietechnologieën, die toereikend zijn om de vertrouwelijkheid van de Vertrouwelijke en Persoonlijke Informatie te beschermen, met dien verstande echter, dat dergelijke encryptie in ieder geval niet minder zal zijn dan de sleutellengte van 2048 bits voor asymmetrische encryptie. Regelmatig draadloze toegangspunten scannen, identificeren en uitschakelen.

13. Verbindingsvereisten

13.1 in het geval Verkoper in samenhang met de Overeenkomst verbinding heeft, of zal krijgen, met Vertrouwelijke en Persoonlijke Informatie, in aanvulling op het voorgaande: Als Verkoper een verbinding heeft of krijgt met de omgeving van CWT, zal Verkoper ten minste:

a. alleen de onderling overeengekomen faciliteiten en verbindingsmethoden gebruiken om de omgeving van CWT te koppelen aan de bronnen van Verkoper;
b. GEEN koppeling tot stand brengen met de omgeving van CWT zonder voorafgaande schriftelijke toestemming van CWT;
c. CWT tijdens normale kantoortijden toegang bieden tot alle toepasselijke faciliteiten van Verkoper, voor het onderhoud en de ondersteuning van apparatuur (bijv. router) die onder de Overeenkomst door CWT is verstrekt voor verbinding met de Vertrouwelijke en Persoonlijke Informatiebronnen;

d. alle onder de Overeenkomst door CWT verstrekte apparatuur gebruiken voor verbinding met de omgeving van CWT, enkel voor het leveren van die diensten en producten of werkzaamheden die expliciet in de Overeenkomst zijn geautoriseerd;
e. als de overeengekomen verbindingsmethode vereist dat Verkoper een Security Gateway implementeert, logs bijhouden van alle sessies die gebruikmaken van een dergelijke Security Gateway. Deze sessielogs moeten voldoende gedetailleerde informatie bevatten om de eindgebruiker of applicatie, het bron-IP-adres, het bestemmings-IP-adres, de gebruikte poorten/serviceprotocollen en de toegangsduur te identificeren. Deze sessielogs dienen na het creëren van de sessie minimaal zes (6) maanden te worden bewaard;
f. CWT toestemming geven om informatie te verzamelen betreffende toegang, inclusief toegang van Verkoper, tot de omgeving van CWT. Deze informatie mag zonder nadere kennisgeving worden verzameld, bewaard en geanalyseerd door CWT voor het identificeren van eventuele veiligheidsrisico's. Deze informatie kan gegevens bevatten van traceringsbestanden, statistieken, netwerkadressen, en de feitelijke gegevens of schermen waartoe toegang is verkregen of die zijn overgebracht;
g. elke verbinding met de omgeving van CWT onmiddellijk opschorten of beëindigen als Verkoper van mening is dat er sprake is van een inbreuk of ongeautoriseerde toegang of in opdracht van CWT als CWT, naar eigen goeddunken, van mening is dat er sprake is van een inbreuk op de beveiliging of ongeautoriseerde toegang tot of verkeerd gebruik van gegevensfaciliteiten van CWT of informatie, systemen of andere bronnen van CWT.

14. Mobiele en Draagbare Apparaten

Verkoper zal ten minste:

14.1 gebruikmaken van volledige, Krachtige Encryptie en geen Persoonlijke Informatie en Vertrouwelijke Informatie op Mobiele en Draagbare Apparaten is opgeslagen opslaan;

14.2 gebruikmaken van Sterke Encryptie om de Vertrouwelijke en Persoonlijke Informatie te beschermen die wordt overgebracht met gebruikmaking van of waartoe op afstand toegang is verkregen door netwerkbewuste Mobiele en Draagbare apparaten.

a. Wanneer gebruik wordt gemaakt van netwerkbewuste Mobiele en Draagbare Apparaten die geen laptops zijn voor toegang tot en/of het opslaan van de Vertrouwelijke en Persoonlijke Informatie, moeten deze apparaten het vermogen hebben om alle opgeslagen kopieën van de Vertrouwelijke en Persoonlijke Informatie te verwijderen na ontvangst via het netwerk van een goed geauthenticeerde opdracht. (Noot: Een dergelijk vermogen wordt vaak een "remote wipe"-vermogen genoemd.)
b. Over gedocumenteerde gedragsregels, procedures en normen beschikken om ervoor te zorgen dat de Geautoriseerde Partij die fysieke controle uitoefent over een netwerkbewust mobiel en draagbaar apparaat dat geen laptop is en waarop Vertrouwelijke en Persoonlijke Informatie is opgeslagen, onmiddellijk start met het verwijderen van alle Vertrouwelijke en Persoonlijke Informatie als het apparaat kwijtraakt of wordt gestolen.
c. Over gedocumenteerde gedragsregels, procedures en normen beschikken om ervoor te zorgen dat Mobiele en Draagbare Apparaten die geen laptop zijn en niet

netwerkbewust zijn, automatisch alle opgeslagen kopieën van de Vertrouwelijke en Persoonlijke Informatie zullen verwijderen na opeenvolgende mislukte inlogpogingen;

14.3 over gedocumenteerde gedragsregels, procedures en normen beschikken die ervoor zorgen dat alle Mobiele en Draagbare Apparaten die worden gebruikt om toegang te krijgen tot de Vertrouwelijke en Persoonlijke Informatie en/of dit op te slaan:

a. in het fysieke bezit van Geautoriseerde Partijen zijn;
b. fysiek beveiligd zijn als ze niet in het fysieke bezit van Geautoriseerde Partijen zijn; of
c. hun gegevensopslag onmiddellijk en veilig laten verwijderen als ze noch in het fysieke bezit van een Geautoriseerde Partij noch fysiek beveiligd zijn, of na 10 mislukte toegangspogingen;

14.4 voorafgaand aan het toestaan van toegang tot de Vertrouwelijke en Persoonlijke Informatie die is opgeslagen op of door middel van het gebruik van Mobiele en Draagbare Apparaten, beschikken over en gebruikmaken van een proces dat ervoor zorgt dat:

a. de gebruiker een Geautoriseerde Partij is die geautoriseerd is voor een dergelijke toegang; en
b. de identiteit van de gebruiker is geauthenticeerd;

14.5 een beleid implementeren dat het gebruik verbiedt van Mobiele en Draagbare Apparaten die niet geadministreerd en/of beheerd zijn door Verkoper of CWT voor toegang tot en/of het opslaan van de Vertrouwelijke en Persoonlijke Informatie;

14.6 ten minste jaarlijks het gebruik van, en controles voor, alle door Verkoper geadministreerde of beheerde Mobiele en Draagbare Apparaten beoordelen, om ervoor te zorgen dat de Mobiele en Draagbare Apparaten kunnen voldoen aan de toepasselijke Technische en Organisatorische Veiligheidsmaatregelen.

15. Beveiliging onderweg

Verkoper zal ten minste:

15.1 gebruikmaken van Krachtige Encryptie voor de overdracht van de Vertrouwelijke en Persoonlijke Informatie buiten door CWT of Verkoper beheerde netwerken of als de Vertrouwelijke en Persoonlijke Informatie wordt overgedragen via een niet-vertrouwd netwerk;

15.2 bestanden met Vertrouwelijke en Persoonlijke Informatie op papier, microfiche of elektronische media die fysiek worden overgedragen, laten vervoeren door een betrouwbare koerier of via een andere leveringsmethode die kan worden getraceerd en veilig laten verpakken volgens de specificaties van de fabrikant. Alle Vertrouwelijke en Persoonlijke Informatie dienen in afgesloten verpakkingen te worden vervoerd.

16. Beveiliging bij Opslag

Verkoper zal ten minste:

16.1 gebruikmaken van Krachtige Encryptie om Vertrouwelijke en Persoonlijke Informatie te beschermen wanneer deze zijn opgeslagen;

16.2 Vertrouwelijke of Persoonlijke Informatie niet elektronisch opslaan buiten de netwerkomgeving van Verkoper (of het eigen veilige computernetwerk van CWT), tenzij het opslagapparaat (bijv. back-up tape, laptop, geheugenstick, computerdisk, etc.) met Krachtige Encryptie is beveiligd;

16.3 Vertrouwelijke of Persoonlijke Informatie niet op verwijderbare media opslaan (bijv. USB flashdrives, thumbdrives, geheugensticks, tapes, cd's of externe harddrives) behalve voor back-up, bedrijfscontinuïteit, een noodherstelplan en gegevensuitwisselingsdoeleinden die zijn toegestaan en vereist op grond van een contract tussen de Verkoper en CWT. Als verwijderbare media worden gebruikt om Vertrouwelijke of Persoonlijke Informatie op te slaan op grond van de uitzonderingen die in deze subafdeling worden genoemd, moet de informatie worden beschermd aan de hand van Krachtige Encryptie. Autorun moet voor verwijderbare media en opslagapparaten worden uitgeschakeld;

16.4 Vertrouwelijke of Persoonlijke Informatie op papier of microfiche op passende wijze opslaan en beveiligen in ruimtes waartoe alleen geautoriseerd personeel toegang heeft;

16.5 tenzij schriftelijk anders is opgedragen door CWT, bij het verzamelen, genereren of creëren van Vertrouwelijke of Persoonlijke Informatie op papier en in back-up media voor, via of namens CWT of onder de merknaam van CWT ervoor zorgen dat deze informatie Vertrouwelijke of Persoonlijke Informatie zal zijn en, indien dit haalbaar is, deze informatie voorzien van het woord "Vertrouwelijk". Verkoper erkent dat de Vertrouwelijke en Persoonlijke Informatie in eigendom van CWT is en zal blijven, ongeacht het label of de afwezigheid hiervan.

17. Retournering, Bewaring, Vernietiging en Verwijdering

Verkoper zal ten minste:

17.1 op verzoek van CWT of na beëindiging van de Overeenkomst binnen dertig (30) dagen na een dergelijk verzoek of beëindiging van de Overeenkomst en zonder extra kosten voor CWT kopieën verstrekken van elke gevraagde Vertrouwelijke en Persoonlijke Informatie. Alle Vertrouwelijke en Persoonlijke Informatie, inclusief elektronische, papieren en beveiligde back-up-versies, ook binnen negentig (90) dagen na de snelste van de volgende mogelijkheden retourneren, of, naar keuze van CWT, vernietigen: (a) expiratie of beëindiging van de Overeenkomst, (b) het verzoek van CWT om de Vertrouwelijke en Persoonlijke Informatie te retourneren, of (c) de datum waarop Verkoper niet langer de Vertrouwelijke en Persoonlijke Informatie nodig heeft voor het leveren van diensten en producten onder de Overeenkomst;

17.2 in het geval CWT vernietiging als een alternatief voor het retourneren van de Vertrouwelijke en Persoonlijke Informatie goedkeurt, schriftelijk de vernietiging bevestigen door een functionaris van Verkoper te laten verklaren dat de Vertrouwelijke en Persoonlijke Informatie niet-opvraagbaar en niet terug te halen is. Verkoper zal overgaan tot volledige vernietiging van alle kopieën van Vertrouwelijke en Persoonlijke Informatie op alle locaties en in alle systemen waar Vertrouwelijke en Persoonlijke Informatie is opgeslagen, inclusief, maar niet beperkt tot, eerder goedgekeurde Geautoriseerde Partijen. Deze informatie zal worden vernietigd volgens een standaardprocedure van de sector voor volledige vernietiging, zoals DOD 5220.22M of NIST Special Publication 800-88 of door gebruikmaking van een door de fabrikant aanbevolen demagnetiseringsproduct voor het betrokken systeem. Voorafgaand aan een dergelijke vernietiging zal Verkoper alle toepasselijke Technische en Organisatorische Beveiligingsmaatregelen toepassen om de veiligheid, privacy en vertrouwelijkheid van de Vertrouwelijke en Persoonlijke Informatie te beschermen;

17.3 Vertrouwelijke en Persoonlijke Informatie op een zodanige wijze verwijderen dat de informatie niet in een bruikbaar formaat kan worden gereconstrueerd. Documenten, dia's, microfilm, microfiche en foto's dienen verwijderd te worden door cross-cut versnippering of verbranding. Materialen met Vertrouwelijke en Persoonlijke Informatie die zullen worden vernietigd, moeten worden opgeslagen in afgesloten verpakkingen en via een betrouwbare derde partij worden vervoerd.

18. Bestrijding en Kennisgeving van Incidenten

Verkoper zal ten minste:

18.1 beschikken over en gebruikmaken van een Proces en samenhangende procedures voor dergelijke Incidentbeheerprocessen en gespecialiseerde medewerkers inzetten voor dit Proces en de procedures. Onmiddellijk, en in geen geval na meer dan vierentwintig (24) uur, CWT ervan op de hoogte brengen via iRespond@mycwt.com als er sprake is van een vermoedelijke of bevestigde aanval op, onrechtmatige toegang tot, ongeautoriseerde toegang tot, verlies van of een andere inbreuk die betrekking heeft op de informatie, systemen of andere bronnen van CWT;

18.2 na CWT in kennis te hebben gesteld, CWT voorzien van regelmatige statusupdates, inclusief, maar niet beperkt tot, de genomen maatregelen om een dergelijk incident op te lossen en dit tijdens de duur van het incident met tussenpozen en op tijdstippen doen die wederzijds zijn overeengekomen, en zo snel als redelijkerwijs mogelijk is na sluiting van het incident, CWT een schriftelijk verslag doen toekomen met een beschrijving van het incident, de door de Verkoper genomen maatregelen tijdens het oplossen ervan en de plannen van Verkoper voor toekomstige maatregelen om te voorkomen dat een dergelijk incident zich nogmaals voordoet;

18.3 een dergelijke inbreuk op de informatie, systemen of andere bronnen van CWT niet openbaar maken zonder eerst CWT in kennis te stellen en rechtstreeks samen met CWT de toepasselijke regionale, landelijke, staats- of lokale overheidsinstanties of kredietcontrolebedrijven,

personen die zijn getroffen door een dergelijke inbreuk en alle toepasselijke typen media informeren, zoals bij wet vereist;

18.4 over een proces beschikken waarmee medewerkers van Verkoper of Derde Partijen onmiddellijk schending van beveiligingscontroles kunnen identificeren, inclusief de schendingen die staan uiteengezet in deze Informatiebeveiligingseisen. Geïdentificeerde overtreders zullen worden onderworpen aan de toepasselijke disciplinaire maatregelen die onderworpen zijn aan de toepasselijke wetten. Niettegenstaande het voorgaande vallen overtreders onder het gezag van de Verkoper of zijn Derde Partijen. CWT zal niet als werkgever van de werknemers van Verkoper of zijn Derde Partijen worden beschouwd.

19. Bedrijfscontinuïteitsbeheer en Noodherstelplan

Verkoper zal ten minste:

19.1 bedrijfscontinuïteits- en noodherstelplannen ontwikkelen, toepassen, beheren en herzien, teneinde de impact voor CWT van de service of producten van Verkoper te minimaliseren. Dergelijke plannen zullen het volgende bevatten: vastgestelde bronnen met betrekking tot Bedrijfscontinuïteits- en Noordherstelplan-functies, vastgestelde doelstellingen voor de hersteltijd en het herstelpunt, een dagelijkse back-up van gegevens en systemen, externe opslag van back-up media en bestanden, bestandsbescherming en contingentieplannen die beantwoorden aan de vereisten van de Overeenkomst en deze plannen op veilige wijze extern opslaan en ervoor zorgen dat deze plannen voor de Verkoper beschikbaar zijn als dit nodig is;

19.2 op verzoek van CWT een gedocumenteerd bedrijfscontinuïteitsplan aan CWT verstrekken dat garandeert dat Verkoper zijn contractuele verplichtingen onder de Overeenkomst en dit document kan nakomen, inclusief de vereisten van toepasselijke omschrijvingen van werkzaamheden of serviceniveau-overeenkomsten. Deze plannen zullen herstel bewerkstelligen en tegelijkertijd de integriteit en vertrouwelijkheid van de Vertrouwelijke en Persoonlijke Informatie beschermen;

19.3 beschikken over gedocumenteerde procedures voor de veilige back-up en het herstel van de Vertrouwelijke en Persoonlijke Informatie, die minimaal procedures voor het vervoer, de opslag en het verwijderen van de back-up kopieën van de Vertrouwelijke en Persoonlijke Informatie zullen bevatten en, op verzoek van CWT, dergelijke gedocumenteerde procedures aan CWT verstrekken;

19.4 ervoor zorgen dat ten minste wekelijks back-ups van alle Vertrouwelijke en Persoonlijke Informatie worden opgeslagen of software en configuraties voor systemen die worden gebruikt door CWT worden gecreëerd;

19.5 regelmatig, ten minste jaarlijks, of volgend op een belangrijke wijziging in bedrijfscontinuïteits- of noodherstelplannen, dergelijke plannen geheel voor eigen kosten van

Verkoper uitvoerig oefenen. Deze oefeningen zullen een goed functioneren van getroffen technologieën en interne bekendheid met zulke plannen garanderen;

19.6 op verzoek onmiddellijk zijn bedrijfscontinuïteitsplan herzien om aanvullende of zich voordoende bedreigingsbronnen of -scenario's aan de orde te stellen en CWT binnen een redelijk tijdsbestek een overzicht van hoog niveau van plannen en testen verstrekken;

19.7 ervoor zorgen dat alle locaties van Verkoper of door Verkoper gehuurde locaties waar zich Vertrouwelijke en Persoonlijke Informatie bevindt of wordt verwerkt 24 uur per dag en zeven (7) dagen per week worden gemonitord op indringing, vuur, water en andere milieurisico's.

20. Naleving en Accreditatie

Verkoper zal ten minste:

20.1 volledige en nauwkeurige bestanden met betrekking tot zijn prestaties of zijn verplichtingen die voortvloeien uit deze Informatiebeveiligingseisen en de naleving van Verkoper hiervan bewaren in een format dat beoordeling of audit mogelijk zal maken, voor een periode van niet minder dan drie (3) jaar of langer als vereist kan zijn ingevolge een gerechtelijk bevel of een civiele of regulerende procedure. Niettegenstaande het voorgaande zal Verkoper alleen vereist zijn om beveiligingslogs gedurende minimaal één (1) jaar te bewaren na doorlopende prestaties uit hoofde van deze overeenkomst;

20.2 het CWT toestaan, zonder extra kosten voor CWT, na redelijke voorafgaande kennisgeving, periodieke veiligheidsbeoordelingen of -audits van de door Verkoper gebruikte Technische en Organisatorische Beveiligingsmaatregelen uit te voeren, gedurende welke CWT aan Verkoper schriftelijke vragenlijsten en verzoeken om documentatie zal verstrekken. Verkoper zal, indien van toepassing, voor alle verzoeken ook een schriftelijk antwoord en bewijs verstrekken, onmiddellijk of, als dit redelijkerwijs niet mogelijk is, na onderlinge overeenstemming. Nadat CWT om een audit door CWT heeft verzocht, zal Verkoper een veiligheidsaudit plannen die binnen tien (10) dagen na een dergelijk verzoek van start gaat. CWT kan toegang vragen tot faciliteiten, systemen, processen of procedures om de beveiligingsbeheeromgeving van Verkoper te kunnen beoordelen;

20.3 op verzoek van CWT bewijs van naleving onder de voorwaarden van dit document verstrekken, inclusief ondersteunende certificaten voor de recentste versies van PCI-DSS, ISO 27001/27002, SOC 2, of een gelijksoortige beoordeling voor de Verkoper. Als de Verkoper niet in staat is om bewijs van naleving te leveren, dan zorgt deze voor een schriftelijk rapport met daarin aangegeven waarin nog geen sprake is van naleving en hoe dit wel gerealiseerd kan worden;

20.4 in het geval dat CWT, naar eigen goeddunken, van oordeel is dat zich een inbreuk op de beveiliging heeft voorgedaan, die niet onmiddellijk overeenkomstig deze Overeenkomst en het Proces voor Incidentbeheer van Verkoper aan CWT is gerapporteerd, de start van de audit of beoordeling plannen binnen vierentwintig (24) uur na de kennisgeving van CWT dat een beoordeling of audit is vereist;

20.5 binnen dertig (30) dagen na ontvangst van de uiteindelijke beoordelingsresultaten of het auditrapport een schriftelijk rapport aan CWT verstrekken, met een overzicht van de corrigerende maatregelen die Verkoper heeft geïmplementeerd of voorstelt te implementeren en met het schema en de huidige status van elke corrigerende maatregel. Dit rapport elke dertig (30) kalenderdagen voor CWT bijwerken en de status van alle corrigerende maatregelen middels de implementatiedatum rapporteren. Alle corrigerende maatregelen binnen negentig (90) dagen na de ontvangst door Verkoper van het beoordelings- of auditrapport implementeren of binnen een alternatief tijdsbestek, mits dit alternatieve tijdsbestek wederzijds en schriftelijk door de partijen is overeengekomen binnen maximaal dertig (30) dagen na de ontvangst door Verkoper van het beoordelings- of auditrapport;

20.6 thans de toepasselijke, door de overheid opgelegde informatiebeveiligingsnormen en rapporteringseisen en ISO 27001/27002 naleven en deze blijven naleven. Voor zover Verkoper betaalrekeningnummers of andere samenhangende betaalinformatie verwerkt, zal Verkoper thans de actueelste versie van Payment Card Industry (PCI-DSS) naleven voor de volledige omvang van systemen die deze informatie verwerken en deze blijven naleven. In het geval Verkoper PCI-DSS niet langer naleeft voor een deel of de volledige omvang van de systemen die op PCI toepasselijke gegevens verwerken, zal CWT onmiddellijk CWT in kennis stellen, onmiddellijk en zonder onnodig uitstel overgaan tot het verhelpen van deze niet-naleving, en op verzoek regelmatig de status van deze oplossing aan CWT verstrekken.

21. Normen, Best Practices, Voorschriften en Wetten

Indien de Verkoper Vertrouwelijke of Persoonlijke Informatie die betrekking heeft op medewerkers en partners van CWT, klanten van CWT of medewerkers, contractanten, subcontractanten of leveranciers van klanten van CWT verwerkt, er toegang tot heeft, of deze informatie bekijkt, opslaat of beheert, zal de Verkoper Technische en Organisatorische Veiligheidsmaatregelen toepassen die niet minder strikt zijn dan wordt vereist door toepasselijke mondiale, regionale, landelijke, staats- en lokale richtsnoeren, voorschriften, richtlijnen en wetten.

22. Wijziging

CWT behoudt zich het recht voor om deze Informatiebeveiligingseisen van tijd tot tijd bij te werken of te wijzigen door de laatste versie op de website van CWT te plaatsen.

Versie 5.0.aff
Datum: april 2024