# VERWERKERSOVEREENKOMST TIMETELL B.V.

*TimeTell Online*

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

*Public register of Data Pro Code: https://scope-europe.eu/en/data-pro-code/public-register*

*Adherence ID: 2023SCOPE6009000DATAPRO*

Versie *1.9 oktober 2023*

# DEEL 1: DATA PRO STATEMENT

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de verwerkersovereenkomst voor het product of de dienst van het bedrijf dat dit Data Pro Statement heeft opgesteld.

## Algemene informatie

1. Dit Data Pro Statement is opgesteld door:

   TimeTell B.V., gevestigd en kantoorhoudend te 2274 KV Voorburg aan de Willem de Bijelaan 147, verder te noemen TimeTell.

   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met de privacy officer: 070-311 48 11 of privacyofficer@timetell.nl

2. Dit Data Pro Statement geldt vanaf de datum waarop de Overeenkomst is getekend door Opdrachtgever

   De in dit Data Pro Statement omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van data protectie steeds voorbereid en actueel te blijven. Wij houden u op de hoogte van nieuwe versies via onze normale kanalen.

3. Dit Data Pro Statement is van toepassing op de volgende diensten van TimeTell (Data Processor)

   TimeTell Online.

4. Omschrijving diensten

   TimeTell Online is een online (SaaS) applicatie ter ondersteuning van werkprocessen in de zakelijke markt. Het product is samengesteld uit specifieke modules voor de discipline tijdregistratie met optioneel: verlof- en ziekteregistratie, plannings- en declaratiegegevens, agendabeheer en budgettering ten behoeve van de zakelijke markt.

5. Beoogd gebruik

   Product is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken: urenregistratie-, plannings- en declaratiegegevens gekoppeld aan minimaal de medewerkersnaam. Optioneel kunnen ook diverse andere gegevens, waaronder persoonsgegevens (zoals NAW-gegevens, functie, schaal en salaris) worden geregistreerd.

Bij TimeTell Online is rekening gehouden met de verwerking van optionele bijzondere persoonsgegevens en zogenoemde 'gevoelige gegevens' (zoals bijvoorbeeld salarisgegevens). Verwerken van deze gegevens met het hiervoor omschreven product of dienst door Opdrachtgever is ter eigen beoordeling door Opdrachtgever.

6. Data Processor heeft bij het ontwerpen van het product/de dienst *privacy by design* op de volgende wijze toegepast:

   Bij de inrichting van TimeTell Online zijn zogenoemde gevoelige gegevens, waaronder bijzondere persoonsgegevens, alleen zichtbaar indien men is gekoppeld aan het juiste autorisatieprofiel van gebruikers bij Opdrachtgever. Tevens wordt aan Opdrachtgever gemeld welke velden in TimeTell Online bijzondere persoonsgegevens bevatten, zoals bedoeld in artikel 9 van de AVG. Deze velden zijn individueel aanvullend te autoriseren en staan in de standaard profielen default op 'niet geautoriseerd'. Data Processor controleert de door Opdrachtgever in TimeTell Online ingevoerde gegevens niet en zal de gegevens uitsluitend inzien op verzoek van klant, bijvoorbeeld in het kader van onderhoud en support aan Opdrachtgever.

7. Data Processor gebruikt de Data Pro Standaardclausules voor verwerkingen.

8. Data Processor verwerkt de persoonsgegevens van zijn Opdrachtgevers binnen de EU/EER.

9. Data Processor maakt gebruik van de volgende sub-processors:

   De infrastructuur dienstverlening (IaaS) is uitbesteed aan Avantage, welke gebruik maakt van meerdere, geografisch gescheiden datacenters van Uniserver. Avantage beschikt over de certificering ISO 9001, ISO 27001, NEN 7510. Uniserver beschikt over ISO 27001 en tevens over een ISAE 3402-verklaring. Deze toont mede aan dat belangrijke aspecten rondom kwaliteit en informatiebeveiliging binnen de gehele bedrijfsvoering worden doorgevoerd. Data processor staat ervoor in dat met de sub-processor een verwerkersovereenkomst is afgesloten met vergelijkbare verplichtingen en waarborgen.

10. Data Processor ondersteunt Opdrachtgever op de volgende manier bij verzoeken van betrokkenen:

    Opdrachtgever heeft zelf volledige toegang tot de gegevens in TimeTell Online en kan deze middels zowel standaard als maat rapportages zelf ontsluiten, bewerken, corrigeren of verwijderen.

11. Na beëindiging van de overeenkomst met een Opdrachtgever verwijdert Data Processor de persoonsgegevens die hij voor Opdrachtgever verwerkt in principe uiterlijk binnen 1 maand na beëindiging contractperiode op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).

    De klantcontactgegevens worden tot maximaal 2 jaar na beëindiging van de hoofdovereenkomst bewaard.

12. Op verzoek van Opdrachtgever kan de Data Processor, na beëindiging van de overeenkomst met Opdrachtgever, alle persoonsgegevens die hij voor Opdrachtgever verwerkt op de volgende manier retourneren:

    Vanaf de dag van beëindiging van de contractperiode is toegang tot de betreffende klantomgeving voor de Opdrachtgever niet meer mogelijk. Opdrachtgever heeft zelf gedurende de contractperiode volledige toegang tot de gegevens in TimeTell Online en kan deze gegevens middels zowel standaard als maat rapportages zelf ontsluiten, bewerken, corrigeren of verwijderen.

    Op verzoek kan Data Processor aanvullend een export van de database als XML of CSV-bestand leveren tegen het op dat moment geldende consultancy tarief. Een dergelijk bestand wordt op de dag van beëindiging van de contractperiode beschikbaar gesteld aan Opdrachtgever.

## Beveiligingsbeleid

1. Data Processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:

    Deze maatregelen staan beschreven in het TimeTell informatiebeveiligingsbeleid. Een kopie van dit document kan op aanvraag worden verstrekt.

## Datalekprotocol

1. In geval er toch iets mis gaat, hanteert Data Processor het volgende datalekprotocol om ervoor te zorgen dat verwerkingsverantwoordelijke op de hoogte is van incidenten:
    - Data Processor beschikt intern over een datalekprotocol om beveiligingsincidenten te managen;
    - Communicatie met Opdrachtgevers en externe partijen is in deze procedure opgenomen.
    - Indien Data Processor zich bewust is geworden van een beveiligingsincident, wordt dit, zonder onredelijke vertraging, binnen 24 uur gemeld aan de bij ons bekende contactpersoon van Opdrachtgever.
        - Contactpersonen betreffen geregistreerde applicatiebeheerders en optioneel een door de opdrachtgever aan te geven privacy contactpersoon.
    - Elk groot incident wordt door Data Processor achteraf geëvalueerd (Post Mortem) met als doel de procedures te optimaliseren en de geleerde lessen te verankeren in de organisatie.
    - Alle informatiebeveiligingsincidenten worden door Data Processor geregistreerd in een Incidentenlogboek.

# INFORMATIEBEVEILIGINGSBELEID TIMETELL B.V.

| Versie | Datum | Auteur | wijzigingen |
|---|---|---|---|
| 2022-1 | 20-5-2022 | DvD | Algehele herziening n.a.v. ISO27001 certificering |
| 2022-2 | 31-10-2022 | BM | Informatie transport toegevoegd |
| 2023-1 | 3-5-2023 | BM | Gescheiden netwerken bijgewerkt |
| 2023-2 | 24-7-2023 | BM | Classificatie aangepast (documenten naar externen) |

VERTROUWELIJK

# Inhoudsopgave

# 1. Management beleid en informatiebeveiliging

*Doel van het informatiebeveiligingsbeleid*

TimeTell hecht veel belang aan het zorgvuldig omgaan met de gegevens van haar klanten. Het informatiebeveiligingsbeleid geeft inzicht in de inspanningen die TimeTell op dit gebied levert.

Het informatiebeveiligingsbeleid is opgesteld conform de ISO27001 norm en volgt dezelfde opbouw. Waar nodig is dit beleid uitgewerkt in deelbeleid, procedures en werkinstructies.

*Management Statement*

Informatiebeveiliging is een integraal onderdeel van de diensten en producten die TimeTell B.V. aanbiedt. De klanten en de medewerkers van TimeTell moeten erop kunnen vertrouwen dat hun data in veilige handen is en dat er alles aan wordt gedaan om deze te beschermen.
Binnen TimeTell is Informatiebeveiliging een gezamenlijke verantwoordelijkheid van alle medewerkers. Het is opgenomen in de interne processen en procedures en het wordt uitgedragen door het management. Van alle medewerkers wordt verwacht hier naar te handelen en waar nodig te signaleren.

*Informatiebeveiligingsbeleid vaststellen*

Het informatiebeveiligingsbeleid wordt minstens jaarlijks getoetst middels zowel een interne, als ook een externe audit in het kader van de ISO27001 certificering, IB gebeurtenissen die impact hebben op de organisatie en/of voortschrijdend inzicht . Het beleid is geldig totdat het door de directie vervangen wordt door een nieuwe versie dan wel expliciet buiten gebruik wordt gesteld. Iedere TimeTell medewerker dient kennis genomen te hebben van het actuele Informatiebeveiligingsbeleid en deze beleidsregels ook toe te passen in de dagelijkse werkzaamheden.

*Scope van het informatiebeveiligingsbeleid*

TimeTell BV levert software ter ondersteuning van werkprocessen in de zakelijke markt.

De online infrastructuur (IAAS) hiervoor is uitbesteed aan een externe leverancier. De eisen vanuit dit informatiebeveiligingsbeleid zijn onverkort op hen van toepassing.

Aangezien er meerdere partijen zijn, die deze online infrastructuur kunnen leveren, is er geen afhankelijkheid van deze leverancier en is er geen sprake van een leveringsketen.

Dienstverlening op locatie valt expliciet onder het informatiebeveiligingsbeleid van de betreffende klant.

## 2. Interne Organisatie

*Rollen en verantwoordelijkheden*

TimeTell is een relatief kleine organisatie met een platte organisatiestructuur. De directie stuurt samen met het management team de medewerkers aan, waarbij op enkele onderdelen gebruikt wordt gemaakt van het 'meewerkend voorman' principe. Voor alle medewerkers, ook onze externe krachten, tenzij anders vermeld, gelden de eisen, zoals vermeld in het TimeTell Arbeidsreglement.

Autorisaties, toegang en definities worden per rol vastgelegd in de TimeTell autorisatiematrix.

Taken en bevoegdheden zijn verder per medewerker vastgelegd in een functieprofiel dat is toegevoegd aan het personeelsdossier van de betreffende medewerker. Specifiek op het gebied van IB beveiliging zijn de rol van SO en PO beschreven en toegewezen aan functionarissen binnen de TT organisatie

Om de scheiding van conflicterende taken en verantwoordelijkheden te waarborgen worden alle autorisatie aanvragen schriftelijk goedgekeurd door een daartoe bevoegd persoon (anders dan de uitvoerder).

*TimeTell User Group*

Om de belangen van gebruikers optimaal te kunnen behartigen is een onafhankelijke gebruikersvereniging opgericht, de TimeTell User Group.

*Project Beheer*

Voor zowel interne als externe projecten dienen de IB-maatregelen meegenomen te worden in het (Sales) proces.

## 3. Mobiele apparaten en telewerken

De voorwaarden bij het gebruik van mobiele apparaten, telewerken en andere IT faciliteiten van TimeTell door medewerkers van TimeTell zijn vastgelegd in het arbeidsreglement van TimeTell.

## 4. Dienstverband

*Screening Personeel*

Alle TimeTell medewerkers dienen een geldige Verklaring Omtrent Gedrag aan te vragen, gericht op bepaalde functieaspecten, die voor TimeTell van belang zijn. De kosten voor de aanvraag worden door TimeTell gedragen.

*Arbeidsvoorwaarden*

Voorwaarden aan dienstverband zijn vastgelegd in het arbeidsreglement en het arbeidscontract.

*Bewustwording en trainingen*

De menselijke factor is de zwakste schakel in IT-security. Security awareness is een methode om medewerkers bewust te maken van de risico's van IT in de dagelijkse praktijk en versterkt het ethisch handelen.

Het security awareness beleid geeft richting aan hoe en aan welke onderwerpen medewerkers getraind moeten worden. Dit beleid is van toepassing op alle medewerkers, inclusief inhuur.

*Vertrouwelijkheid (Privacy of Information)*

Alle TimeTell medewerkers met toegang tot persoons- en/of vertrouwelijke informatie dienen de TimeTell regels inzake vertrouwelijkheid te kennen en toe te passen. Het arbeidsreglement bevat tevens een geheimhoudingsclausule toegespitst op het vertrouwelijk omgaan met klantgegevens en welk disciplinair proces wordt toegepast bij overtreding daarvan. Alle TimeTell medewerkers tekenen dit reglement voor akkoord. Externe inhuur en Auditors tekenen apart een geheimhoudingsovereenkomst.

*Wijziging rol of beëindiging dienstverband*

Bij een wijziging in rol of verantwoordelijkheden, wordt gebruik gemaakt van een aanvraagformulier 'autorisaties' welke door de Technisch Directeur wordt beoordeeld.

Bij beëindiging van een dienstverband wordt gebruik gemaakt van het proces 'werknemer uit dienst'

## 5. Asset management

Alle software, hardware en informatie assets vertegenwoordigen waarde binnen TimeTell.

Informatie over configuratie items, die nodig zijn voor het leveren van de IT diensten/producten, wordt vastgelegd in een inventarisatielijst, welke de installed base voor de beheersing van de IT Infrastructuur vormt. Tevens wordt in deze lijst vastgelegd wie eigenaar is van welk informatiesysteem.

Gebruik, wijzigingen en teruggave van middelen worden gereguleerd vanuit het HR-beleid en via gebruikersovereenkomsten.

## 6. Informatie classificatie

TimeTell heeft de door haar getroffen technische en organisatorische beveiligingsmaatregelen afgestemd op de aard van de, door TimeTell, te verwerken persoonsgegevens ten behoeve van klant. Voor dit doel wordt een verwerkingsregister bijgehouden conform de Europese standaard (AVG).

Tevens dient te worden opgemerkt dat het de verantwoordelijkheid is van klant als verwerkingsverantwoordelijke, zoals bedoeld in de Algemene Verordening Gegevensbescherming om te beoordelen of de in TimeTell Online te verwerken persoonsgegevens mogen worden verwerkt. Binnen TimeTell wordt alle informatie per definitie als vertrouwelijk geclassificeerd. Documenten die we versturen naar externen zijn openbaar tenzij deze het label vertrouwelijk hebben gekregen.

Hogere classificaties zijn aan de orde als de informatie(systemen) persoonsgegevens bevatten. Deze zijn dan uitsluitend toegankelijk op basis van Need to Know en Need to Access. De website en ander marketing- of promotiemateriaal zijn openbaar toegankelijk. In de TimeTell autorisatiematrix wordt bijgehouden wie toegang heeft tot welke informatie en op basis waarvan.

In het arbeidsreglement staat aangegeven hoe medewerkers dit kunnen herkennen.

## 7. Behandeling van Media

Uitgifte van media wordt vastgelegd via gebruikersovereenkomsten. Gebruik en vervoer vindt plaats conform Maatregelen IT Security (onderdeel van Arbeidsreglement).

Voor het afvoeren of overdragen van media geldt:

- Datadragers worden fysiek verwijderd en opgeslagen tot deze vernietigd kunnen worden;
- Hardware wordt afgevoerd en aangeboden bij hiertoe gespecialiseerde bedrijven ter vernietiging;
- Indien media zakelijk over wordt genomen door een collega wordt eventueel aanwezige gebruikersdata geverifieerd verwijderd;
- Indien privé/extern overgenomen vindt een Re-install/fabrieksinstellingen plaats en wordt het apparaat uit het domein gehaald.
- Vertrouwelijke documenten of documenten waarin bijzondere persoonsgegevens vermeld zijn, worden altijd vernietigd met behulp van een papier versnipperaar indien deze documenten niet meer een operationeel belang dienen.

## 8. Toegangsbeveiliging

Het beleid binnen TimeTell is dat toegang tot digitale data en netwerken wordt verstrekt op een ‘Need to Know’ en ‘Need to Access’ basis in lijn met wat noodzakelijk is voor de uitvoering van de werkzaamheden. Dit is verder uitgewerkt in een autorisatiematrix

IaaS dienstverlening ten behoeve van de Online servers

De IaaS dienstverlening is uitbesteed aan een externe partij, die gebruik maakt van een datacenter-onafhankelijke infrastructuur. De afspraken inzake fysieke toegangsbeveiliging tot de IaaS vallen onder de generieke beveiligingsafspraken zoals vastgelegd in de SLA met de externe dienstverlener.

Datacenters

De externe dienstverlener maakt gebruik van meerdere, geografisch gescheiden datacenters in Europa. De maatregelen voor fysieke toegangsbeveiliging tot deze datacenters worden afgedekt door certificering van de externe dienstverlener. Hiermee is aantoonbaar dat belangrijke aspecten rondom kwaliteit en informatiebeveiliging binnen de gehele bedrijfsvoering zijn doorgevoerd.

## 9. Gebruikers Toegangsmanagement

*Gebruikers registratie en toegang:*

Binnen de TimeTell organisatie hebben uitsluitend daartoe bevoegde personen, uit oogpunt van hun rol, toegang tot de productiedatabases. Hiertoe zijn persoonlijke accounts ingericht, waarbij toegang tot de online servers (t.b.v. beheer) uitsluitend vanaf kantoor kan plaatsvinden via een VPN-tunnel. Andere medewerkers hebben geen toegang tot de databases van klanten, maar indien dit nodig is voor het uitvoeren van de werkzaamheden, worden zij door een bevoegd persoon, conform hetgeen gesteld in de TimeTell autorisatiematrix, geautoriseerd voor inzage in TimeTell omgevingen.

Gebruikers (klanten) van TimeTell krijgen uitsluitend toegang tot hun eigen bedrijfsomgeving. Klanten zijn zelf verantwoordelijk voor het regelen van toegang en autorisatie van hun medewerkers tot hun eigen omgeving.

*Beheer toegangsrechten:*

Nieuwe medewerkers krijgen toegang tot de voor hen relevante (netwerk)locaties en systemen middels een aanvraagformulier, welke door HRM wordt aangevraagd en op directieniveau wordt goedgekeurd. Bij het uitdienst treden van medewerkers worden de toegekende autorisaties weer ingetrokken. Het tussentijds toekennen van aanvullende autorisaties vindt uitsluitend plaats na goedkeuring van de technisch directeur en worden toegekend door de SO. Alle autorisaties worden geëvalueerd door SO, PO en directie vertegenwoordiging in het Security Review overleg. Dit overleg wordt minstens 1x per jaar gevoerd en middels notulen vastgelegd.

*Beleid op beheer en gebruik van authenticatie informatie door gebruikers*

- Wachtwoorden zijn in lijn met de aanbevelingen van het CIS en worden afgeschermd opgeslagen in een digitale wachtwoordkluis;
- Individuele inlog wachtwoorden mogen niet gelijk zijn aan de wachtwoorden die de medewerker privé gebruikt;

## 10. Systeem en applicatie toegangscontrole

*Restricties op toegang informatie*

Toegang tot informatie is rol-gebaseerd, waardoor gebruikers alleen toegang hebben tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden, zoals vastgelegd in de autorisatiematrix

*Secure log-on procedures*

Beeldschermen, indien onbeheerd, dienen te worden gelocked (default na 5 minuten geen activiteit) en toegang tot sessies wordt na 3 foutieve inlog pogingen automatisch 15 minuten geblokkeerd

*Systeem voor wachtwoordbeheer*

Het is aan de gebruikers (klant) zelf om verificatie via een wachtwoord in de TimeTell software vast te leggen of om verificatie via de externe authenticatie (ADFS, Azure, etc.) te laten verlopen. Binnen de software heeft de klant mogelijkheden om daarvoor criteria  teconfigureren..

TimeTell Medewerkers maken gebruik van:

- Digitale wachtwoordkluis t.b.v. wachtwoordopslag;
- Hardware token ten behoeve van toegang tot relevante systemen;
- Waar mogelijk wordt er gebruik gemaakt van tweestapsverificatie;
- Werkstations, voorzien van endpoint protection;

*Gebruik van speciale programmatuur*

Alleen vooraf geaccepteerde uitvoerbare programma's mogen gestart worden. Dit wordt softwarematig afgedwongen.

*Toegang tot broncode:*

Het document Software Ontwikkeling beschrijft de procedures rond de ontwikkeling van de TimeTell software. Hierin zijn ook de beveiligingsmaatregelen m.b.t. development en broncode opgenomen. Ook is hierin het release management beschreven.

## 11. Cryptografie

- Encryptie moet worden toegepast op de communicatie en de opslag van gevoelige gegevens.
- Encryptie wordt toegepast op informatie transport van klant gegevens;
- Klantgegevens, die worden opgeslagen op mobiele opslagmiddelen, zoals USB of laptop, moeten versleuteld worden opgeslagen.
- Klantgegevens, die via een koppeling worden uitgewisseld met externe systemen van de klant worden via een beveiligde verbinding met authenticatie verstuurd.

- Versleuteling vindt plaats conform ‘best practices’ volgens de richtlijnen van het National Institute of Standards and Technology (NIST) https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines
- Wachtwoorden voor versleuteling worden opgeslagen in een beveiligde password-manager.

## 12. Veiligheidsgebieden

*Fysieke (toegangs)beveiliging van de kantoor omgeving*

TimeTell medewerkers hebben, afhankelijk van hun functie, fysieke toegang tot ruimten binnen TimeTell. Het proces voor het verstrekken, beheersen en intrekken van fysieke toegang is een belangrijk onderdeel van het totale TimeTell security programma en is verder uitgewerkt in de TimeTell autorisatiematrix

*Beveiliging tegen externe en omgevingsdreigingen*

- De schade door bedreigingen van buitenaf (zoals brand, overstroming, explosies, oproer, stroomonderbreking) wordt beperkt door passende preventieve maatregelen.
- Toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe.
- De uitgifte van toegangsmiddelen wordt geregistreerd.
- In enkele zones van het pand wordt gebruik gemaakt van cameratoezicht. Het gebruik van beeldmateriaal is onder meer beperkt door de Wet bescherming persoonsgegevens.
- Externe (Data)verbindingen worden beschermd tegen interceptie of beschadiging.

## 13. Apparatuur

Er wordt minimaal halfjaarlijks gekeken of er updates beschikbaar zijn gesteld voor de door TimeTell gebruikte systemen, waarna deze worden ingepland. De gebruikelijke Microsoft updates worden na verificatie wekelijks doorgevoerd.

Medewerkers volgen het Clear Desk/Clear Screen principe, zoals ook vastgelegd in het arbeidsreglement. Schermen worden, bij verlaten werkplek, gelocked door de medewerker (tevens automatisch na time-out).

Alle hardware die niet langer noodzakelijk is of in aanmerking komt voor hergebruik, wordt geschoond en informatie wordt vernietigd, alvorens de media af te voeren of opnieuw uit te geven.

Het beleid omtrent de aanschaf van nieuwe software is verder uitgewerkt in de TimeTell procedure Software Acquisitie. Uitgangspunt is dat TimeTell de standaard functionaliteiten van de betreffende software gebruikt en hier geen maatwerk op (laat) toepassen

## 14. Operationele procedures en verantwoordelijkheden

*Change management*

TimeTell is een Off-the-Shelve product, waarbij binnen de bestaande software enige ruimte is voor klantspecifieke inrichting. In het geval dat een specifieke aanpassing door klanten wordt aangevraagd,

is er sprake van een Request for Change.  Change Management beschrijft hoe wijzigingen kunnen worden aangevraagd en vervolgens worden beoordeeld, waarna deze op een gecontroleerde manier in productie worden genomen (software) danwel hoe hardware aanpassingen (infrastructuur) worden doorgevoerd en hoe wordt verzekerd dat uitsluitend geteste en geaccordeerde systemen (hardware en software) in gebruik worden genomen.

*Capaciteitsmanagement*

Servercapaciteit wordt bijgehouden in een interne tool, zodat een capaciteitscheck plaats kan vinden bij het aanmaken/uitbreiden van klantomgevingen.

IT-beheer monitort de TimeTell infrastructuur op mogelijke capaciteits- en/of beschikbaarheidsissues. Dit gebeurt met behulp van een serverbeheer tool die alerts stuurt naar IT Beheer. Binnen de monitoring software wordt gebruik gemaakt van tresholds die, indien deze onder of boven een bepaalde waarde uitkomen, een alert uitsturen naar IT Beheer.

*Scheiding van omgevingen*

Het document Software Ontwikkeling beschrijft de procedures rond de ontwikkeling van de TimeTell software. Hierin zijn ook de beveiligingsmaatregelen m.b.t. development en broncode opgenomen. Ook is hierin het release management beschreven.

Voor installatie van Online servers zijn gedetailleerde stappenplannen uitgewerkt. Deze dienen altijd gevolgd te worden. Deze stappenplannen worden onderhouden door IT beheer.

## 15. Bescherming tegen Malware

Er wordt gebruik gemaakt van software tools om te monitoren op, en te beschermen tegen software virussen en malware. Deze software verkrijgt automatisch updates via de leverancier(s) indien nieuwe virusdefinitie files verschijnen of een update van het programma plaatsvindt. Patches, indien beschikbaar, worden handmatig door IT-Beheer geïnstalleerd.

## 16. Back-up & restore

Het is van belang dat ICT systemen en data, die essentiële business functies ondersteunen, in geval van problemen kunnen worden hersteld.

Backup and Restoration ten behoeve van Online omgevingen worden afgedekt door de policies van de externe IaaS dienstverlener.  Afspraken over RPO en RTO zijn contractueel vastgelegd.

Er is een interne backup-procedure voor de klantomgevingen opgesteld, waarbij op verzoek de omgeving tot 7 dagen geleden kan worden terug gezet.

## 17. Logging en monitoring

Activiteiten die gebruikers uitvoeren op de online systemen worden vastgelegd in logbestanden. Hetzelfde geldt voor andere relevante gebeurtenissen, zoals pogingen om ongeautoriseerd toegang te

krijgen en verstoringen die kunnen leiden tot verminking of verlies van gegevens. De logbestanden worden gecontroleerd, zodra er een indicatie is dat een proces onjuist is verlopen of op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de persoonsgegevens.Waar nodig wordt actie ondernomen.

- Servercapaciteit wordt bijgehouden in een dashboard, zodat een capaciteitscheck plaats kan vinden bij het aanmaken/uitbreiden van klantomgevingen;
- IT-beheer monitort de TimeTell infrastructuur op mogelijke capaciteits- en/of beschikbaarheidsissues. Dit gebeurt met behulp van een serverbeheer tool die alerts stuurt naar IT Beheer
- De tool werkt met alerts die verzonden worden bij het ontdekken van (potentiële) problemen. De werking van de tool wordt dagelijks gecontroleerd;
- IT Beheer monitort op pogingen om onrechtmatige toegang te krijgen en monitort verkeerde log-ins. Onregelmatigheden worden gerapporteerd aan de SO;
- Er wordt gemonitord op het toepassen van de security baseline (CIS compliant);
- Alle processen (waaronder backup) worden gemonitord. Onregelmatigheden worden geregistreerd;
- Er zit bewaking op log- en audittrails. Incidenten met betrekking tot ongeautoriseerd toegang of verstoringen, die kunnen leiden tot verminking of verlies van gegevens, worden gerapporteerd aan de SO en behandeld als zijnde een security incident;

TimeTell maakt gebruik van internet tijdservers voor tijdsynchronisatie.

Afspraken rond het installeren van software zijn vastgelegd in het arbeidsreglement en het gebruik ervan staat geregistreerd in de autorisatiematrix.

## 18. Management technische kwetsbaarheden

Beveiligingsmaatregelen worden getroffen op basis van beveiligingsadviezen van het NCSC. Indien een systeem meer maatregelen nodig heeft, wordt een risicoanalyse uitgevoerd.

## 19. Audit Management

TimeTell monitort direct (door middel van  vulnerability scanning en PEN-testing) dan wel indirect (via interne en externe audits in het kader van ISO27001 certificering) of de genomen maatregelen voor informatiebeveiliging correct geïmplementeerd en werkend zijn. Waar nodig maakt TimeTell gebruik van het recht om bij externe partners de informatieveiligheidswerkzaamheden te bezien (right to audit).

## 20. Netwerk beveiligingsmanagement

*Geïmplementeerde maatregelen op netwerken*

- Toegang tot interne wifi-netwerken is alleen beschikbaar voor specifieke apparaten, op basis van goedkeuring;
- Externe toegang tot de kantoor omgeving is uitsluitend mogelijk via een VPN-verbinding;

- Beheer van Online servers is uitsluitend mogelijk vanaf het kantoor netwerk.

*Beveiligen van netwerk services*

- Externe verbindingen zijn beveiligd middels een firewall;
- Extern toegankelijke diensten zijn uitsluitend via beveiligde (VPN) verbindingen benaderbaar;

*Scheiding in netwerken*

- Netwerksegmenten worden zoveel mogelijk gescheiden om ongewenste onderlinge communicatie te voorkomen.

## 21. Informatie overdrachten

Afspraken over op welke wijze gegevens overdracht mag en kan plaatsvinden, evenals afspraken over geheimhouding zijn vastgelegd in het Arbeidsreglement.

## 22. Acquisitie, ontwikkeling en onderhoud IT systemen

Op acquisitie en ontwikkeling van interne IT-systemen is de procedure Inkoop Management van toepassing.

Er worden, indien beschikbaar gesteld door de leverancier(s), updates uitgevoerd op interne IT-systemen.

## 23. Beveiliging in test- ontwikkeling- en support processen

In het deelbeleid Software Ontwikkeling is het volledige proces beschreven zoals dit wordt toegepast voor de ontwikkeling van de TimeTell software. Deze documentatie behelst zowel het ontwikkelbeleid, het test-, change- en release management en geïmplementeerde control procedures. Hierin zijn ook de beveiligingsmaatregelen m.b.t. development en broncode opgenomen. Ook is hierin het release management beschreven.

## 24. Leveranciers service delivery management

TimeTell maakt gebruik van partners voor het beheer van de online infrastructuur (IaaS). In contracten en SLA’s met deze partners worden de TimeTell eisen op het gebied van informatiebeveiliging vastgelegd. TimeTell monitort direct (zelfstandig) dan wel indirect (via externe audit rapporten) de naleving. Waar nodig maakt TimeTell gebruik van het recht om bij de partners de informatieveiligheidswerkzaamheden te bezien (right to audit).

Alle SLA’s en contracten dienen getekend te zijn door zowel de partners als TimeTell en worden jaarlijks geëvalueerd.

## 25. Management van informatiebeveiligingsincidenten

- TimeTell maakt gebruik van registratiesystemen om vragen en incidenten vast te leggen;
- TimeTell heeft een incidenten procedure om zware beveiligingsincidenten te managen. De directie is eigenaar van deze procedure en verantwoordelijk voor de juiste en volledige implementatie;
- Communicatie met klanten en eventuele externe partijen ten aanzien van beveiligingsincidenten is in het beleid (en bijbehorende instructies) opgenomen;
- Elk groot incident wordt achteraf geëvalueerd (post mortem) met als doel de procedures te optimaliseren en de geleerde lessen te verankeren in de organisatie;
- Alle informatiebeveiligingsincidenten worden geregistreerd in het TimeTell Incidenten logboek;
- Incidenten waarbij sprake is van een inbreuk op persoonsgegevens worden tevens gelogd in een datalekkenregister.
- Bij incidenten, waarvan sprake is van een inbreuk op persoonsgegevens, wordt in team-overleg (PO, SO en Technisch Directeur) besloten welke passende rol de vervolgstappen neemt en contact onderhoudt met de betreffende instanties.
- In het geval van IB incidenten die een hoge mate van risico omvatten, wordt het Informatiebeveiligingsbeleid beschouwd om te beoordelen of aanvullend beleid nodig is. Tevens wordt de risico analyse beschouwd om te beoordelen of de getroffen maatregelen nog adequaat zijn of een aanpassing nodig hebben.

## 26. Bedrijfscontinuïteitsplan

TimeTell hecht belang aan continuïteit en heeft daarom een bedrijfscontinuïteitsplan opgesteld

Continuïteit van de software is gewaarborgd via een ESCROW overeenkomst met de TimeTell User Group en de Escrow Alliance waarin periodiek de meest actuele software release wordt overgedragen.

## 27. Naleven wettelijke en contractuele eisen

TimeTell streeft ernaar om in al haar processen en procedures te voldoen aan de relevante wet- en regelgeving. Dit doet zij op basis van het principe “Pas toe of leg uit”.

## 28. Informatie beveiliging beoordelingen

Informatie beveiligingsbeoordelingen vinden plaats door middel van jaarlijkse interne en externe audits. De rapportages die deze audits opleveren worden binnen directie en (security)management besproken. Op basis van beschreven bevindingen worden acties ondernomen om deze bevindingen te adresseren. De Security Officer is hierin leidend