Whitepaper: Continuïteit & Beveiliging van TotalDesk Datacenter- en Werkplekdiensten

Hoe TotalDesk beschikbaarheid, integriteit en vertrouwelijkheid borgt—van datacenter tot moderne werkplek

Versie 1.2 | Januari 2026

Managementsamenvatting

Organisaties vertrouwen dagelijks op digitale diensten die altijd beschikbaar moeten zijn en aantoonbaar veilig moeten blijven. TotalDesk borgt de continuïteit en beveiliging van haar datacenter- en werkplekdiensten met een samenhangende set van organisatorische, technische en fysieke maatregelen. Daarbij staan risicogestuurd werken, transparantie richting klanten en toetsbare processen centraal, ondersteund door een ISO/IEC 27001-certificering met jaarlijkse audits. Met een eigen Security Operations Center (SOC) monitort TotalDesk de beveiliging 24x7 en kan er (waar passend) automatisch worden ingegrepen bij verdachte activiteiten. Voor herstelbaarheid voert TotalDesk dagelijkse back-ups uit op disk, aangevuld met een offline (airgapped) back-up op tape als extra beschermingslaag. Deze whitepaper beschrijft op hoofdlijnen hoe TotalDesk de beschikbaarheid, integriteit en vertrouwelijkheid van klantdata en -diensten waarborgt—van redundante infrastructuur en back-up tot identity security (zoals MFA), monitoring en herstelprocedures.

Kernmaatregelen in één oogopslag:

- ISO/IEC 27001-gecertificeerd, met jaarlijkse audits
- Dubbele uitvoering en redundantie over gescheiden datacenterlocaties
- Dagelijkse back-ups op disk, aangevuld met airgapped back-ups op tape
- 24x7 security monitoring via eigen SOC met (waar passend) geautomatiseerde respons
- Sterke identity security, waaronder MFA en ‘least privilege’

Scope en uitgangspunten

Deze whitepaper geeft een beknopt en zakelijk overzicht van maatregelen waarmee TotalDesk de continuïteit en beveiliging van haar diensten borgt. De beschreven maatregelen zijn gericht op:

- **Beschikbaarheid**: hoge uptime door redundantie, failover en aantoonbare herstelbaarheid.
- **Integriteit**: bescherming tegen ongeautoriseerde wijziging en aantoonbare juistheid van configuraties en data.
- **Vertrouwelijkheid**: toegang uitsluitend voor geautoriseerde personen en systemen, met sterke identiteits- en toegangscontrole.
- **Risicogestuurde aanpak**: maatregelen worden ontworpen, beoordeeld en verbeterd op basis van risico's en impact.
- **Gedeelde verantwoordelijkheid**: TotalDesk beveiligt de onderliggende platformen en beheerde diensten; klanten blijven verantwoordelijk voor keuzes in gebruik, data-classificatie en (waar van toepassing) eindgebruikersgedrag en applicaties.

Governance, compliance en ISO 27001

TotalDesk beschikt over een ISO/IEC 27001-certificering en wordt hiervoor jaarlijks geaudit. De certificering is gebaseerd op een Information Security Management System (ISMS) waarmee informatiebeveiliging structureel is ingericht als een continu proces van beleid, risicoanalyse, implementatie, toetsing en verbetering.

- **Beleid en procedures** voor o.a. toegangsbeheer, wijzigingsbeheer, incidentmanagement en back-up & herstel.
- **Risicomanagement** met periodieke beoordeling van dreigingen, kwetsbaarheden en impact op diensten.
- **Interne controles en audits** inclusief jaarlijkse (externe) ISO 27001-audits om naleving en effectiviteit van maatregelen te toetsen.
- **Leveranciers- en ketenbeheer**: selectie, beoordeling en afspraken over beveiliging en continuïteit binnen de supply chain.
- **Bewustwording** en training voor medewerkers met rollen en verantwoordelijkheden passend bij hun functie.

Datacenterbeveiliging (fysiek en operationeel)

De beveiliging van datacenteromgevingen start met fysieke maatregelen die ongeautoriseerde toegang voorkomen en operationele continuïteit ondersteunen. TotalDesk past hierbij het principe van ‘defense-in-depth’ toe: meerdere lagen van beveiliging die elkaar versterken.

- **Toegangscontrole** met registratie en autorisatie voor datacentertoegang, conform ‘least privilege’.
- **Cameratoezicht en logging** van relevante toegangsmomenten.
- **Omgevingsbeveiliging** zoals branddetectie/-preventie, klimaatbeheersing en gecontroleerde stroomvoorziening.
- **Operationele procedures** voor wijzigingswerkzaamheden, onderhoud en escalaties om risico’s op verstoringen te beperken.

Continuïteit door redundantie: dubbele uitvoering van datacenters

Om uitval te minimaliseren is de infrastructuur zodanig ontworpen dat kritieke componenten geen single point of failure vormen. Waar mogelijk zijn voorzieningen dubbel uitgevoerd en verdeeld over gescheiden datacenterlocaties, zodat onderhoud en incidenten gecontroleerd kunnen worden opgevangen.

- **Gescheiden datacenters** voor spreiding van risico’s (bijv. stroom, brand, locatie-incidenten).
- **Endpoint protection/EDR** (detectie en respons op endpointniveau) ter bescherming tegen malware en verdachte activiteiten.
- **Onderhoud met minimale impact** door gepland onderhoud, change control en gecontroleerde failover waar van toepassing.
- **Capaciteitsmanagement** om piekbelasting en groei op te vangen zonder service degradatie.

Back-up, herstel en ransomware-weerbaarheid

Back-up en herstel zijn essentieel voor bedrijfscontinuïteit—zeker bij incidenten zoals ransomware, menselijke fouten of technische storingen. TotalDesk voert dagelijkse back-ups uit op disk voor snel herstel en maakt daarnaast een offline (airgapped) back-up op tape als aanvullende waarborg tegen sabotage of encryptie.

- **Dagelijkse back-up op disk** voor snelle restores en operationeel herstel.
- **Airgapped back-ups op tape** als aanvullende beschermingslaag (offline/gescheiden van het primaire netwerk) om herstel mogelijk te houden, ook bij ransomware of gerichte sabotage. Op verzoek kunnen klanten hun eigen data op eigen tapes binnen hun eigen locatie bewaren.
- **Retentiebeleid** afgestemd op klantbehoefte en compliance-eisen (bewaartermijnen en versies).
- **Herstelprocedures en periodieke restore-tests** om te verifiëren dat back-ups daadwerkelijk bruikbaar zijn.
- **RPO/RTO-afspraken** (Recovery Point/Time Objective) afhankelijk van dienst en SLA, zodat verwachtingen vooraf helder zijn.

Identity & Access Management (IAM): MFA en 'least privilege'

Een groot deel van incidenten start bij identiteit: gestolen wachtwoorden, misbruik van accounts of te ruime rechten. TotalDesk beveiligt toegang tot beheer- en klantomgevingen met sterke identiteitscontroles en het principe van minimale rechten.

- **Multi-Factor Authentication (MFA)** voor beheeraccounts en waar passend voor eindgebruikers, om risico's van wachtwoordmisbruik te reduceren.
- **Role-Based Access Control (RBAC)** en scheiding van taken (Segregation of Duties) voor beheertaken.
- **Privileged Access** met extra waarborgen voor admin-rechten (bijv. aparte beheeraccounts, extra logging en striktere policy).
- **Joiner/Mover/Leaver processen** voor tijdige aanmaak, wijziging en intrekking van rechten.
- **Toegangsreviews** om periodiek te controleren of rechten nog passend zijn.

Netwerk- en platformbeveiliging

TotalDesk past technische maatregelen toe om aanvallen te voorkomen, laterale beweging te beperken en afwijkend gedrag snel te detecteren. De inrichting is gebaseerd op gelaagde beveiliging (preventie, detectie en respons) en bewezen ontwerpprincipes.

- **Netwerksegmentatie** om klantomgevingen, beheer en back-upstromen logisch te scheiden en impact van incidenten te beperken.

- **Next-generation firewalling** en filtering op inkomend/uitgaand verkeer, met beleid gebaseerd op ‘deny by default’ waar passend.
- **Veilige beheerkanalen** (bijv. afgeschermde management-netwerken en streng gecontroleerde remote access).
- **Versleuteling** waar relevant voor data in transit en/of at rest, afhankelijk van dienst en architectuurkeuzes.
- **Hardening** van systemen en platformen (beperken van services, veilige configuratiebaselines).

Monitoring, logging en incidentrespons

Beveiliging is niet alleen preventie. Continue monitoring en een strak incidentproces zorgen ervoor dat verdachte activiteiten snel worden opgespoord en adequaat worden opgevolgd. TotalDesk voert deze bewaking uit via een eigen Security Operations Center (SOC) dat 24x7 zicht houdt op relevante signalen en gebeurtenissen. TotalDesk legt relevante events vast en gebruikt deze voor detectie, forensische analyse en continue verbetering.

- **Eigen SOC (24x7)** voor continue bewaking en snelle opvolging, met (waar passend) geautomatiseerde acties en playbooks om risico’s direct te beperken.
- **Centrale logging** van kritieke platform- en security-events (o.a. authenticatie, privilege-activiteiten, configuratiewijzigingen).
- **Alerting en opvolging** op basis van use-cases en drempelwaarden, met duidelijke escalatieroutes.
- **Incidentmanagement** met triage, containment, eradication en recovery, inclusief communicatie-afspraken richting klanten.
- **Lessons learned** en structurele verbetermaatregelen na incidenten.

Kwetsbaarheden, patching en wijzigingsbeheer

Het tijdig verminderen van kwetsbaarheden vraagt om controle over configuraties en wijzigingen. TotalDesk combineert change management met patch- en vulnerability-processen om risico’s te beperken zonder de stabiliteit van diensten te ondermijnen.

- **Patchmanagement** met geplande onderhoudsvensters en prioritering op basis van impact en dreigingsniveau.
- **Vulnerability management** (signalering en beoordeling van kwetsbaarheden, inclusief mitigaties wanneer patchen niet direct mogelijk is).

- **Wijzigingsbeheer** met risico-inschatting, test/validatie en rollback-scenario's om verstoringen te voorkomen.
- **Configuratiebeheer** om inzicht en consistentie in platformconfiguraties te borgen.

Beveiligde moderne werkplek

Naast datacenterdiensten levert TotalDesk werkplekdiensten waarin eindpunten (laptops, desktops en mobiele apparaten) veilig beheerd worden. Door consistente policies en proactieve beveiliging wordt het risico op datalekken en accountmisbruik verminderd.

- **Device management** met beleid voor configuraties, compliance en lifecycle (uitrol, vervanging, afvoer).
- **Endpoint protection/EDR** (detectie en respons op endpointniveau) ter bescherming tegen malware en verdachte activiteiten.
- **Versleuteling van apparaten** waar van toepassing om risico's bij verlies/diefstal te beperken.
- **Veilige toegang** tot bedrijfsapplicaties met policy-gestuurde controles (bijv. MFA/conditional access afhankelijk van scenario).
- **Standaardisatie** van werkplekken en applicatieconfiguraties om beheerbaarheid en veiligheid te verhogen.

Business Continuity & Disaster Recovery (BC/DR)

Continuïteit vraagt om voorbereiding op incidenten met grotere impact. TotalDesk onderhoudt herstelplannen en procedures die zijn afgestemd op de kritikaliteit van diensten, met als doel dienstverlening gecontroleerd te herstellen binnen afgesproken termijnen.

- **DR-runbooks** met concrete stappen voor herstel en failover per dienst/component.
- **Scenario-denken** (bijv. datacenterstoring, ransomware, grote configuratiefout) inclusief prioritering van herstel.
- **Periodieke tests en oefeningen** om aannames te valideren en procedures te verbeteren.
- **Communicatieafspraken** richting klanten bij incidenten (statusupdates, impact, verwachte hersteltijd).

Transparantie richting klanten

Vertrouwen ontstaat door aantoonbaarheid. TotalDesk communiceert helder over verantwoordelijkheden, serviceafspraken en beveiligingsmaatregelen, en ondersteunt klanten bij vragen vanuit audits of compliance-trajecten.

- **SLA- en beschikbaarheidsafspraken** passend bij de gekozen dienst.
- **Beveiligingsdocumentatie** en (waar van toepassing) audit- en certificeringsinformatie ter ondersteuning van klantvragen.
- **Duidelijke security contactpunten** voor incidentmeldingen, vragen en afstemming.

Conclusie

TotalDesk borgt continuïteit en beveiliging met een gelaagde aanpak: governance volgens ISO 27001-principes, fysieke en technische beveiligingsmaatregelen, redundante datacenterinrichting, dagelijkse back-ups met een airgapped kopie, sterke identiteitsbeveiliging (MFA) en aantoonbare herstelprocedures. Daarmee biedt TotalDesk een robuust fundament voor betrouwbare datacenter- en werkplekdiensten, zodat klanten zich kunnen richten op hun kernprocessen.

Vervolgstap

Wilt u toetsen hoe deze maatregelen aansluiten op uw risico's, compliance-eisen en gewenste RPO/RTO? TotalDesk licht graag de mogelijkheden toe en kan desgewenst een dienst- en risicoanalyse uitvoeren als basis voor een passend beveiligings- en continuïteitsniveau.