safespring

POLICYDOKUMENT:

Säkerhet & hållbarhet på Safesprings datacenter

Din säkra källa för infrastrukturtjänster

Miljö och hållbarhet

Att värna om miljön är för oss en självklarhet. Våra tjänster produceras i miljöeffektiva datahallar och vi på Safespring har ett hållbart arbetssätt.

Hela 100 procent av energin till våra datahallar kommer från förnybara källor, såsom vatten, vind och solkraft. Energi är en grundläggande komponent i de tjänster som vi erbjuder våra kunder. Vi tar miljöhoten på allvar och lägger mycket engagemang i att hela tiden utveckla nya sätt att förbättra design och drift av våra datacenter och hur vi som medarbetare reser inom tjänsten. Det här betyder att vi alltid försöker optimera energieffektivitet samt minska koldioxidutsläpp och avfall från vår verksamhet.

Det här är Safespring

Safespring erbjuder en storskalig molnplattform som lyder under svenska lag. Vi har erbjudit moderna infrastrukturtjänster sedan 2014.

Våra kunder ställer höga krav på säkerhet samtidigt som de efterfrågar flexibilitet, vilket inte alltid är enkelt att åstadkomma lokalt hos dem. Safespring erbjuder ett lättanvänt gränssnitt där lagring, kraftfullare virtuella servrar och säker backup kan beställas med ett knapptryck och tas tillvara på direkt utan några ställtider. Det är stor skillnad mot att behöva beställa ny hårdvara och installera lokalt för kunden. Vi låter med andra ord kunden fokusera på sitt arbete och inte på verktygen. Lika enkelt kan de skala ner när de inte behöver lika mycket resurser längre vilket gör det mer ekonomiskt.

Hos Safespring lämnar data aldrig landet. Säkerheten och stabilitet i vår produktion har gjort att många kunder inom hälso-, sjukvård, forsknings- och akademisk sektor och andra branscher valt Safespring som sin molntjänstleverantör.

Safesprings moderna plattform ger dig möjlighet att skapa en säker applikation.

Safesprings säkerhetspolicy

Vi ställer höga krav på våra datacenter. Våra datacenter följer MSBs klass 3 rekommendationer för datacenter eller har högre motsvarande skydd.

PLACERING AV UTRYMMET Utrymmet ska inte placeras i omedelbar anslutning till våtutrymmen eller större elektromagnetiska källor, exempelvis hissmaskinrum. Placering vid yttervägg samt under markplan bör undvikas. Utrymmet ska vidare inte placeras i närheten av förvaring av brandfarligt material eller i närheten av förvaring av brännbara material som kan agera katalysator vid en eventuell brand, t.ex. kontorsförråd. Utrymmet bör placeras minst en våning över markplan. Omkringliggande vattendrag eller andra risker för inströmmande vätska ska tas hänsyn till.

BYGGNATION OCH SKALSKYDD Utrymmet ska minst uppfylla kraven i SSF 200, skyddsklass 3 för konstruktion, fastsättning av golv, väggar, tak och dörrar. Samtliga väggar ska ansluta tätt till golv och tak. Fönster ska inte finnas i utrymmet. Det bör finnas operatörsrum/ arbetsrum i anslutning till utrymmet (lämpligen i en sluss).

BRANDSKYDD Utrymmet ska utgöra en egen brandcell och uppfylla brandteknisk klass minst EI60 men bör uppfylla brandteknisk klass EI-120. Vid svårigheter att minimera brandbelastning eller motsvarande situationer ska högre brandtekniska klasser som exempelvis R60/90D utredas.

GOLV Installationsgolv med antistatisk matta (även kallat datagolv) ska användas, med en höjd på minst 400 mm över underliggande golv. Det ska finnas lyftanordningar för att möjliggöra släckning av kabelbränder under golv. Det bör finnas fluorescerande riktningsmarkeringar på golven som visar vägen till utrymningsutgångar.

TAK Ljudabsorbenter eller undertak ska undvikas för att inte binda eller samla damm.

DÖRRAR Utrymmet ska vara utformat med en sluss om två dörrar. Slussen ska ha en yta om minst fem till sex kvadratmeter, för att tillåta förvaring av papper/böcker/ manualer/licenser eller annat brännbart material som inte ska förvaras inne i utrymmet. Stålдörrar som minst uppfyller motståndsklass 4 enligt SS EN1627 samt utrymmets brandtekniska klass (se brandskydd) ska användas. Alla dörrar ska av utrymningsskäl öppnas utåt. Låscylindrar ska ingå i den egna verksamhetens låssystem. Låsningen ska vara separerad på sådant sätt att endast behörig personal bereds tillträde.

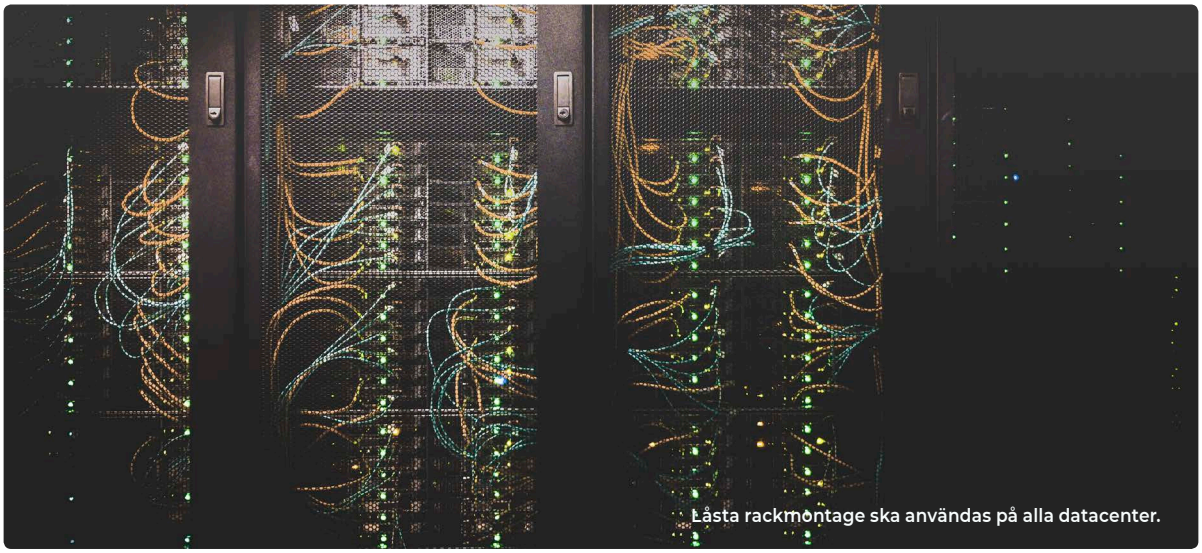
TILLTRÄDE Tillträde ska endast vara tillåtet för behörig personal. Tillträdeskontroll ska ske genom passagekontrollsystem med loggfunktion.

INBROTTSLARM Alla dörrar ska vara larmade och larmen kopplade till verksamhetens ordinarie larm-övervakning. Utrymmet ska utgöra ett eget larmområde enligt SSF 130, minst larmklass 2, larmklass 3 bör användas.

NÖDSIGNAL, ÖVERFALLSLARM Det bör finnas lättåtkomliga olycksfalls- och överfallslarm inom utrymmet vilka är anslutna till verksamhetens ordinarie larmövervakning.

EL Elkraftssystemen som försörjer utrymmet ska vara av typen 5-ledarsystem. Två separata elkraftsmatningar inklusive huvudbrytare och centraler bör användas. Överspänningsskydd ska finnas för all infrastruktur i utrymmet såsom elkraftsförsörjning, kylanläggning och telekommunikation.

Reservkraft ska finnas. Reservkraft ska även mata klimatanläggning, belysning samt allmänkraft i utrymmet. Varje stativ för it-utrustning ska förses med avbrottsfri kraft (UPS), minst två separata grupper per stativ med 2 X 16A trefas på handske. UPS av typen on-line ska användas. En riskanalys ska göras


Låsta rackmontage ska användas på alla datacenter.

för att fastställa om dubbla UPS behövs. Varje UPS (om dubblerad) bör ha sitt eget batteri. Belysningen, övriga eluttag eller annan allmänkraft i utrymmet ska matas från en grupp som är skild från UPS. Separat avsäkrade fördelare (PDU) ska användas i stativ.

Batterier för UPS bör vara ventilreglerade och bör ha en förväntad livslängd på minst 10 år. Batterierna ska vara dimensionerade för att säkerställa el under den tid som åtgår för kontrollerad avstängning av utrustningen alternativt manuell start av reservkraft, dock minst 10 minuter och maximalt 30 minuter. Batterierna bör placeras på en fristående ställning men kan även vara integrerade i UPSanläggningen. Observera att öppna batterier kräver ett eget utrymme samt att batteripaket kan ge stor punktlast vilket kan kräva förstärkningar av golv.

Riskanalyser ska utföras för att fastställa elanläggningarnas behov av kompletterande åtgärder.

EMP (ELEKTROMAGNETISK STRÅLNING) Behovet av skydd mot elektromagnetisk strålning ska utredas.

BELYSNING Medelbelysningsnivå bör vara 500 lux. Lysrörsarmaturer anpassade till känsliga miljöer ska användas. Utrymmet ska utrustas med säkerhetsbelysning som dimensioneras för funktion under minst en timme. Eventuella utgångsskyltar ska lysa kontinuerligt. Behovet av nödbelysning ska utredas.

KORSKOPPLING Korskopplingar för allmänt datanät i fastigheten bör inte finnas i utrymmet, utan placeras till separata utrymmen.

KANALISATION Separata kabelstegar för el- och datanät ska användas. Vid nyanläggning ska 50 % reservutrymme för utbyggnad och komplettering planeras.

GENOMFÖRINGAR Alla kabel- och rörgenomföringar ska vara brandtätade enligt utrymmets brandtekniska klass (se brandskydd). Användning av flexibla genomföringar ska övervägas.

MONTAGE Rackmontage ska användas.

SEPARATA PLACERINGAR It-utrustning för säkerhetskopiering ska placeras i en brandcell som är skild ifrån it-utrustning som lagrar primärdata. Reservkraft och utrustning för automatiska släcksystem samt klimatanläggning ska placeras i separata utrymmen.

VÄTSKA Rörledningar och övriga installationer som innehåller vätska, utöver de som är nödvändiga för klimatregleringen, ska inte finnas i utrymmet. Dragning av rörledningar ska i största möjliga mån göras under installationsgolv. Om vätskeinstallationer finns i utrymmet ska avloppsbrunnar finnas. Anläggning av avlopps- brunn ska även övervägas vid låg


100% av elen till våra datacenter kommer från förnyelsebar energi.

placering och vid risk för inströmmande vätska. Avloppsbrunnar ska ha skydd mot uttorkning och mot uppstigande vätska. Fuktlarm ska finnas och larmet ska vara anslutet till verksamhetens ordinarie larmövervakning.

KLIMAT Utrymmets temperatur ska inte tillåtas variera utanför temperaturgränserna +18 °C till +23 °C. Utrymmet ska förses med ventilations- och kylanordning (av typ precisionskyla). Underblåsande kyla ska användas. Ventilations- och/ eller klimatanläggning ska producera ett övertryck. Temperaturlarm, kopplat till verksamhetens ordinarie larmövervakning, ska finnas. En anordning för reglering av utrymmets luftfuktighet ska användas. Risker för vätskeläckage från kylanordning ska tas hänsyn till.

Tilluft samt luft som passerar klimatutrustning ska filtreras. Dessa filter ska bytas regelbundet. Tilluftskanaler ska förses med rökdetektorer anslutna till brandspjäll eller automatiska fläktstopp. Luftomsättningen ska dimensioneras utifrån arbetsmiljökraven för att det antal personer som är tänkta att kunna vistas kontinuerligt i utrymmet. Nödkyla (ytterligare köldbärare) ska finnas tillgänglig för att säkerställa kontinuerlig drift. Kyleffekten hos kylanordningen för utrymmet ska utredas men bör dimensioneras med minst 2 kilowatt per kvadratmeter yta.

BRAND Brandlarm med egen larmsektion som är kopplat till verksamhetens ordinarie brandlarmsövervakning ska finnas. Det ska finnas handbrandsläckare (typ av släckmedel som inte skadar it-utrustning), innehållande minst 5 kilo släckmedel, både på utsidan av utrymmet i nära anslutning till ordinarie ingång samt inne i utrymmet. Om ventilationsanläggning finns, ska ventilationskanaler förses med brandspjäll kopplade till brandlarm. Utrymmet ska förses med ett automatiskt brandsläckningssystem med aspirerande/samplande branddetektering. Samtliga dörrar ska förses med panikregel på insidan. Material inne i utrymmet ska inte vara brännbart. Detta gäller t.ex. hyllor, stativ, skåp eller andra montage eller möbler som används.

SEKTIONERING Utrymmet bör efter behov kunna sektioneras, exempelvis för utrustning med olika krav på tillträdesskydd eller skalskydd. Om sektionering används ska alla områden avskärmas, inklusive krypgrunder, ventilationsgångar och under installationsgolv. Sektionering ska uppfylla de krav som ställs för skyddsklass 2 i SSF 200. Observera att sektionering också kan utföras för att skapa separata brandceller i utrymmet för att på så sätt minska kraven på släckanläggningens storlek och mängden släckmedel.

SKYLTNING Skyltning utanför utrymmet som avslöjar utrymmets funktion eller innehåll ska undvikas. Rutiner/regler som gäller för utrymmet bör skyltas tydligt inne i utrymmet.

MÄRKNING All utrustning ska märkas med varaktigt märksystem. Alla skyltar ska sättas fast med skruv, nit eller band. Alla hållare för utbytbar märkning ska sättas fast med motsvarande metod. All märkning ska byggas upp med anläggningsnummer i kombination med text eller löpnummer. Märkningen ska inte följa med exempelvis täcklock eller frontplåt när dessa avlägsnas. Märkning ska göras på samtliga ledningar vid centralutrustning, vid anslutningsobjekt samt vid varje passage av överspänningsskydd eller brandcellsgräns samt valv- och markgenomgång.

LEDNINGAR OCH KABLAR Kabelgravar utanför skalskyddsgränsen bör undvikas. Kabelbrunnar bör förses med lås. Jordnings- och potentialskillnadsproblem ska ägnas stor uppmärksamhet, speciellt om anläggningen ska anslutas till befintlig kanalisations- och kabelinfrastruktur.

INSATSPLANER OCH UTRYMNINGSPLANER Alla utrymmen ska ha en giltig och uppdaterad insatsplan för brand, vätskeläckage, sabotage eller andra tillbud (definierade i riskanalys). Insatsplanen för brand ska uppfylla SBF 100 och bör uppfylla kraven i SBF 110.

ALLMÄNNA UTRYMMEN Ingången är skyddad av vakt. Datacentret tillhandahåller ett offentligt kundområde med kontorsfaciliteter och tillgång till kaffe etc. för kundens slutanvändare, som arbetar i datacentret.

ANLÄGGNINGENS INTRÄDE TILL KUNDERS DATACENTEROMRÅDEN Datacentret kan bara kommas åt genom en sluss, för att komma igenom slussen krävs en personlig bricka med biometri-teknik. Kundrollen ”Change List Authoriser” är ansvarig för att ge tillgång till kundområden, både permanent och tillfällig tillgång.

ANLÄGGNINGENS INTRÄDE TILL GEMENSAMMA DATACENTEROMRÅDEN Ytterligare säkerhetsnivåer kan införas som låsbara burar eller kuber (inneslutningsgångar). Kundrollen ”Change List Authoriser” är ansvarig för att ge tillgång till kundområden, både permanent och tillfällig tillgång.

SÄKER PERSONALZON Tillgång till kontor är begränsad utanför kontorstid, bevakas av vakter på plats och övervakas 24/7.

LEVERANSOMRÅDE Datacentret är utrustade med en separat lastbrygga, där kapacitet för stor mängd utrustning behövs.

BSI ISO 22301
Business Continuity Management

BSI ISO 27001
Information Security Management

Våra datacenters säkerhet

Våra datacenter är Co-locations, och säkrade av vakter, som är permanent närvarande på plats dygnet runt, året runt.

SÄKERHETSRUNDOR / EXTERNA PATRULLER
Lokalerna patrulleras av säkerhetsvakter, patrullerna utförs 24/7 och täcker alla områden; kundrum, infrastrukturområden och utomstående områden.

VIDEOÖVERVAKNING Områdena är skyddade av Closed-Circuit Television (CCTV) och övervakade dygnet runt, året runt av säkerhetsvakter. Videoövervakning utförs med två ändamål:

1) Förebyggande av brott - Begränsa risken för stöld och risk för infrastruktur
2) Övervaka och skydda personer, som arbetar i säkra områden

Övervakning aktiveras på uppdrag av respektive datacenter inom och utanför byggnaden på alla säkra områden och andra strategiska områden inom datacentret - inte i kundrum.

Övervakning aktiveras 24/7, men inspelningar görs endast när rörelse detekteras av systemet. Kvaliteten på inspelningen utförs enligt specifikationerna.
Övervakning genomförs enligt gällande lag "*Kamerabevakningslag (2018: 1200)*" Inspelningarna lagras i 30 dagar.

INSPELNINGAR / KONTROLLER Tillgången till poster är begränsad. Vid brottsutredning kontrolleras materialet och kan överlämnas till polisen för vidare utredning. Under extern revision kommer det att vara tillåtet att titta på inspelningar, där revisor eller datacentrets personal är synlig - för att dokumentera att inspelningarna existerar.

EXTERN REVISION AV SÄKERHETEN Säkerheten styrs som en del av SOC2-granskningen. Du kan se ytterligare beskrivning i SOC: s revisionsrapport - avsnitt 3.3.2.5 här nedan:

CC5.5 - KONTROLL B: Datacentrets fysiska säkerhet innefattar, men är inte begränsat till, följande:

1) Säkra rum, burar och skåp med nycklar eller access-märken
2) Övervakningskameror som täcker hela omkretsen (i och runt byggnaden)
3) Larmsystem (ljud och bild)
4) Infraröda sensorer
5) Säkerhetspersonal på plats 24/7
6) Redundanta utåtgående telefonlinjer
7) Årliga revisioner utförs på fysisk säkerhet för datacentret.

CONTROL CC7.1A Loggnings- och övervakningsmjukvara används för att samla in data om säkerhets- och tillgänglighetsbrott och incidenter på grund av skadliga handlingar, naturkatastrofer eller fel. Vid överträdelser och incidenter utförs lämplig uppföljning.


Datacentren är bevakade med CCTV.

Fysiskt åtkomst

Våra datacenter är co-locations vilket ökar den fysiska säkerheten och skapar skydd i flera lager.

Det elektroniska ID-kort, som alla permanenta kortinnehavare får, måste bäras synliga. Tillgångstillståndet är individuellt och beviljas de som fått ID-kort av en behörig på datacentrets co-location. Kundtillgång till säkra områden kräver alltid användning av access-kort, en personlig PIN-kod och biometrisk data.

TILLGÅNG TILL DATACENTER / SÄKRA OMRÅDEN Vår tillgång till Datacentren - Under genomförandeperioden tilldelar Safespring personer som får rollen som ”Change List Authorisers”, som kan tillhandahålla och ändra alla tillstånd för vår räkning.

KONTINUERLIGA KONTROLLER Safespring är ansvarig för att ge tillgång och granska den beviljade åtkomsten. Vår ändringslista auktoriserare har alltid fullständig synlighet för den beviljade åtkomsten via kundportalen.

PERSONAL OCH LEVERANTÖRERS TILLGÅNG TILL DATA CENTER Datacenter-anställd och leverantörens fysiska tillgång till anläggningarna, kundrummen och Datacenterområdena är begränsad till auktoriserad personal och är baserad på arbetsfunktion. Verkställande direktören ansvarar för att tillåta tillgång till Datacenterområden.

Tillgång till leverantörer beviljas av den ansvariga beställaren. Leverantörsansvarig måste ha tydligt synliga ID-kort och identifiera sig hos datacentrets säkerhetspersonal. Arbetsorderna bärs av leverantörens anställd för att dokumentera sitt utseende i Datacentret.

KONTINUERLIGA KONTROLLER Säkerhetsnivåer och åtkomst granskas periodiskt.

BESÖKARE Alla besökare måste meddelas i förväg av den ansvariga auktoriseraren. Besökare måste tillhandahålla bevis på identitet med nationellt ID, körkort eller pass och kontrolleras mot fördefinierade behörighetsåtkomstlistor. Besökare är inloggade, övervakas av videokameror och måste ha ett personligt åtkomstmärke, såvida inte datacentrets säkerhetspersonal är närvarande. ID-kort måste bäras tydligt synliga, och besökare måste identifiera sig hos datacentrets säkerhetspersonal när de begär det.

EXTERN REVISION AV FYSISK ÅTKOMST
Fysisk åtkomst styrs som en del av SOC2-granskningen. Du kan se ytterligare beskrivningar i SOC Audit report – section 3.3.2.5:

CONTROL CC,5,5A Det finns formella förfaranden för att ge tillgång till datacentret för tillfälliga entreprenörer och besökande kunder. Dessa förfaranden innefattar, men är inte begränsade till, följande:

1) Process för att begära tillgång till datacentret
2) Identifiering på entreprenadens sida mot registrerat ID
3) Enhetsmatris som visar alla begränsade områden
4) Husregler som måste läsas innan du går in på plats

CONTROL CC5.5C Alla nya, ändrade eller återkallade permanenta fysiska åtkomsträttigheter begärs genom en central process som hanteras av datacentrets europeiska kundservicecenter (EKSG). Tillgången valideras av en EKSG-agent innan åtkomst beviljas.

KONTINUITETSKONTROLLER / "BLACK BUILDING TEST" För att säkerställa hållbarhet och utveckling av kontinuitetsplanen måste det - åtminstone en gång per år - genomföras praktisk träning. Utbildningarna kommer att innehålla olika discipliner och element i affärsplanen.

Utifrån utbildningen och testen skapas utvärderingsrapporter och identifierade områden för förbättring dokumenteras och en plan för genomförande kommer att utvecklas. Resultatet av sådana kontinuitetstester diskuteras, de klassificeras som konfidentiella och kan inte kommuniceras till kunder.

EXTERN GRANSKNING AV KONTINUITETSTESTER Kontinuitetstester kontrolleras som en del av SOC2-revisionen. Du kan se ytterligare beskrivningar i specificerade avsnitt:

DESCRIPTION I 3.3.2.13 - CONTROL A1.3 Business Continuity-förfaranden, inklusive återställande av säkerhetskopior, finns på plats och testas årligen för att återställa funktionaliteten vid en katastrof.

EXTERNA REVISIONER Datacentret granskas årligen av externa revisorer - vilket resulterar i en årlig oberoende försäkringsrapport - *SOC2 typ II,* som styr säkerhetsutförandet hos datacentret.

Beskrivningen är avsedd att ge användarna information om moln- och operatörskoncentrationens datacentertjänstersystem, särskilt systemkontroller, som är avsedda att uppfylla kriterierna för säkerhets- och tillgänglighetsprinciperna som anges i TSP-sektion 100, *Trust Services Principles*, Kriterier och illustrationer för säkerhet, tillgänglighet, behandling av integritet, sekretess och sekretess som utfärdats av AICPA: s styrelsekommitté för förvaltningstjänster (tillämpliga förtroendeskriterier).

Rapportens omfattning gäller för de lokala datacenteren. SOC2-ramverket är utvecklat av AICPA för att mäta överensstämmelse med definierade affärsprocesskontroller och är synonymt med ISAE3402 och SSAE16.

Avsnitt III innehåller en systembeskrivning av den övergripande säkerhetsuppsättningen och avsnitt IV med beskrivning av alla kriterier, kontroller, utförda tester och resultat av dessa (typ II).

Den senaste tillgängliga SOC2-rapporten täcker kalenderåret 2018 och släpptes i början av februari 2019.

NUVARANDE ISO-CERTIFIKAT Den senaste ISO-revisionen för Sverige ägde rum i april 2018 som en del av den globala globala certifieringsrunda.

Våra datacenters hållbarhet

Alla Safesprings datacenter arbetar aktivt för en hållbarare produktion. 100 procent förbyelsebara energikällor driver datacentren.

Ett av våra datacener utövar sedan 2015 Fortum Värms kylservice för datacenter. Kyltjänsten med värmeåtervinning ger datacentret med kylt vatten och datacentret returnerar vattnet med en temperatur på minst 24 grader celcius. Erbjudandet omfattar övervakning, larm och serviceavtal.

Kylvattenkylningen och värmeåtervinningen tillhandahålls av Fortum Värms fabrik och levereras via distriktets kylnät. På datacentret är en värmeväxlare, mixer och cirkulationspump allt som krävs för att på ett tillförlitligt sätt kyla datacentret. Den återvunna överskottsvärmen från datacentret går in i stora värmepumpar på Fortum Värms anläggning och skickas vidare till fjärrvärmenätet. På det sättet kan värme som tidigare helt enkelt avvisats i friluft nu värma tusentals bostäder. Alla våra datacenter drivs av 100 procent förnyelsebara energikällor och driver initiativ för en hållbarare produktion. Safespring co-location i Oslo jobbar för att öka vattenkraftdrivna datacenter.

Safesprings anställda sitter utspridda i Sverige och Norge och genomför videomöten inom organisationen och med kunder för att minska resor och klimatpåverkan.

Byggnaderna

Ett av våra datacenter var ursprungligen byggt för tryckeri och därför är konstruktionen extremt robust byggd för att hantera vibrationer och tunga vikter.

Datacentren är byggd som en ”byggnad i en byggnad” med separata väggar och tak som är perimeterarna.

Datacentren är oberoende av hyresvärden på alla områden och har egen strömförsörjning, generatorer och brandinstallation.

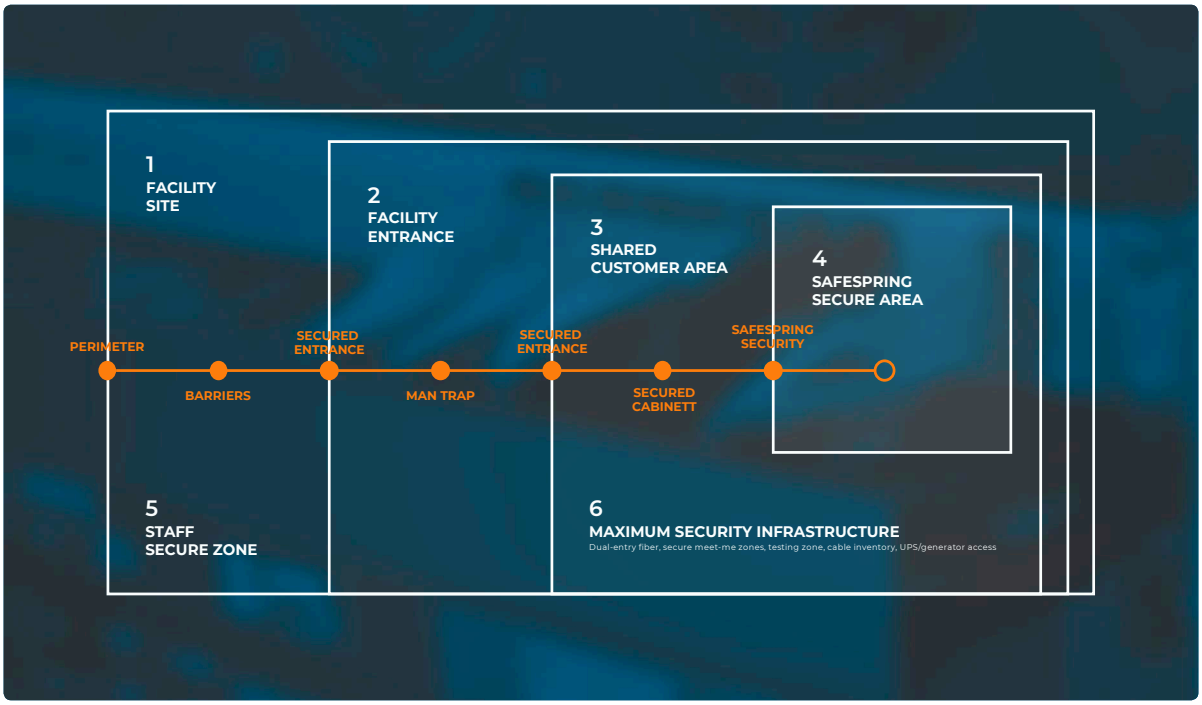
För att möta safesprings SLA är datacentret byggt i enlighet med ”*Design Engineering Requirement*” (DER) som utvecklats av ”*Digital Technology and Engineering Group*” (DTEG), som beskriver standarden för design, byggande och driftsättning.

Under åren har platserna underhållts och uppgraderats för att fullt ut uppfylla kraven. Alla byggnader är indelade i offentliga områden, säkra kundområden och säkra infrastrukturområden.

FLERA SÄKERHETSLAGER Datacentren använder säkerhetsgränser för att skydda områden som innehåller informations- och informationshanteringsanläggningar och säkra områden skyddas av lämpliga inmatningskontroller för att säkerställa att endast behörig personal får tillgång.

När det är möjligt utnyttjas de säkerhetsåtgärder som vidtas, ett skiktat tillvägagångssätt, där kontrollerna blir strängare från den yttersta omkretsen av anläggningen till de inre begränsade utrymmena.

Starka metallfästen ger en säker barriär mot störningar i den privata buren och omgivningen. De privata burarna kan sträcka sig från golvplattan under det upptagna åtkomstgolven och upp till takplattan. De privata burarna använder solida metallpaneler för att dölja visuell inspektion av innehållet.



Safespring Stockholm Norr

Datacentret återvinner värmen som genereas från produktionen tillbaka till fjärrvärmenätet vilket årligen värmer upp tusentals lägenheter i stockholmsområdet.

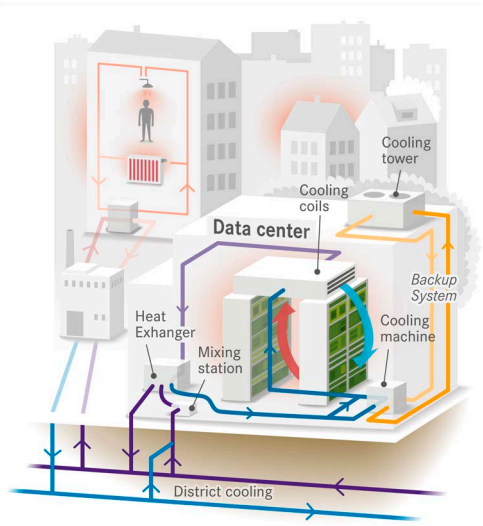
Datacentret är säkrat och byggt som en byggnad, inom en byggnad. Övervakning med CCTV sker dygnet runt alla dagar i veckan och säkerhetsvakter patrullerar området. Det finns flera åtkomsthinder, inklusive slussar, kontaktlösa nyckelkort och biometriska läsare.

Hållbarhet

Safespring Stockholm Norr använder enbart 100 procent grön energi, och har gjort det sedan 2012.

Datacentret har sedan 2015 ett unikt projekt tillsammans med Stockholm Exergi (tidigare Fortum Värme) där de återvinner värme från datacentret till fjärrvärmenätet. Årligen värmen detta upp tusentals lägenheter i Stockholm.

Utvecklingen för mer energieffektiva datacenter pågår ständigt vilket medför att det genomförs löpande förändringar i designen av datacenter, detta inkluderar bland annat: Höjt golvet i datacentren från 60 cm till 120 centimeter för att minska behovet av kylning.



Datacentret genererar värme till stadsdelen.

Safespring Compute

Safespring Storage

Synkzone by Safespring


Datacentret drivs till 100 procent med el från förnyelsebara energikällor.

Safespring Stockholm Syd

Safespring Stockholm Syd matchar höga krav på driftsäkerhet och tillgänglighet.

Datacentret i är idag 2800 kvm stort varav 1100 kvm är datazoner. Datacentret drivs till 100 procent med el från förnyelsebara energikällor och ständigt arbetas det med att hitta nya sätt att öka energieffektiviteten.

Datacentrets ansvarige kan göra utdrag på passersystem och kameramaterial om vi skulle önska det. Safesprings utrymmen är låsta så det går inte att påverka eller manipuleras av någon utomstående.

Byggstandarden är designad för tillgänglighetskrav enligt Tier-3 som är Safesprings policy. Det finns även ett reservkraftsystem som gör datavcentret oberoende av elnätet.

Datacentret har branddetektering med luftanalys. Serverhallar med IT-vänliga släcksystem och brandlarm direktkopplat till brandstation och inbrottslarm direktkopplat till larmcentral samt övervakning 24/7 av egen NOC.

Övrigt

- UPS med N+1 eller 2N
- Kylsystem med N+1 eller 2N
- Design för 1,2-1,3 i energieffektivitet (PUE)
- Förberedda för energiåtervinning

Safespring Backup

Safespring Storage

Safespring Oslo

Den här fastigheten är det största befintliga datacentret i Norge och drivs av vattenkraft.

Datacentret kommer att samarbeta med flera parter för att underlätta vattenkraftgenererade datacenter till nationella och internationella kunder.

Den här fastigheten är det största befintliga datacentret i Norge. Ledande internationella datacenters operatörer hyr ca. 6 000 m2 i byggnaden. Fastigheten har 22 MW kraftkapacitet installerad och potentialen att expandera för datacenter operatörer är stor. Byggnaden är totalt 25 000 kvadratmeter. Safespring producerar Compute, och Storage i det här datacentret.

Safespring Compute

Safespring Storage

Datacentret ”Safespring Oslo” drivs av vattenkraft.

Safespring är din säkra källa för infrastrukturtjänster

Besök gärna vår webbplats för att lära dig med om molntjänster och hur Safespring kan lösa dina behov av Backup, Storage och Compute.

www.safespring.com

safespring

+46 (0)8-55 10 73 70 | info@safespring.com
Smidesvägen 12, 171 41 Solna, Sweden

www.safespring.com