



**احداث دیتاسنتر تخصصی گرید Tier III با قابلیت ارتقا به Tier IV و ارائه جامع‌ترین خدمات زیرساخت ابری،
میزبانی، پردازش داده و امنیت سایبری در منطقه آزاد شهر فرودگاهی امام خمینی (ره)**

Construction of Tier III (Upgradable to Tier IV) Specialized Data Center and Provision of
Comprehensive Cloud Infrastructure, Hosting, Data Processing and Cybersecurity
Services in Imam Khomeini Airport City Free Zone with Approximately 4000 Square Meters
of Built-up Area



این مستند صرفاً به عنوان معرفی و تشریح با موضوع مذکور در منطقه آزاد شهر فرودگاهی امام خمینی (ره) بوده و سرمایه‌گذاران محترم می‌بایست در طرح خود، اطلاعات و ارقام پیشنهادی مندرج در این مستند را بررسی، بروزآوری، تدقیق و جرح و تعدیل نمایند.

This document is intended solely as an introductory and descriptive overview of the investment opportunity pertaining to the aforementioned subject within the Free Zone of Imam Khomeini Airport City. Esteemed investors are respectfully advised that, in formulating their respective investment proposals, they bear the sole responsibility to independently examine, update, verify, and, where deemed necessary, critically reassess and adjust the indicative information, data, and figures contained herein.

بخش اول: عنوان فرصت سرمایه گذاری

عناوین فارسی و انگلیسی طرح:

عنوان فارسی کامل: احداث دیتاستر تخصصی گرید Tier III با قابلیت ارتقا به Tier IV و ارائه جامع ترین خدمات زیرساخت ابری، میزبانی، پردازش داده و امنیت سایبری در منطقه آزاد شهر فرودگاهی امام خمینی (ره)

English Title: Construction of Tier III (Upgradable to Tier IV) Specialized Data Center and Provision of Comprehensive Cloud Infrastructure, Hosting, Data Processing and Cybersecurity Services in Imam Khomeini Airport City Free Zone

کد شناسایی طرح:

نوع طرح:

طرح زیرساختی-خدماتی در حوزه فناوری اطلاعات و ارتباطات با ماهیت ترکیبی (ساخت، بهره برداری، ارائه خدمات ارزش افزوده دیجیتال و همکاری های استراتژیک بین المللی)

مقیاس طرح (حجم سرمایه گذاری):

چهل و پنج میلیون یورو که به صورت مرحله ای و بر اساس فازبندی اجرایی تزریق خواهد شد. این مبلغ شامل سرمایه اولیه احداث ساختمان و زیرساخت های فیزیکی دیتاستر، تأمین تجهیزات تخصصی سرور، شبکه و ذخیره سازی، هزینه های اخذ گواهینامه های بین المللی و استانداردهای امنیتی، سرمایه در گردش عملیاتی سه سال اول، هزینه های جذب و آموزش نیروی انسانی متخصص، هزینه های تحقیق و توسعه در حوزه های بهینه سازی مصرف انرژی و امنیت سایبری، و هزینه های بازاریابی و جذب مشتریان استراتژیک داخلی و بین المللی می باشد.

افق زمانی بهره برداری:

- فاز صفر (مطالعات تفصیلی فنی-اقتصادی، اخذ مجوزهای حاکمیتی و محیط‌زیستی، و انتخاب پیمانکاران): ۸ ماه از

تاریخ تصویب طرح

- فاز یک (عملیات عمرانی، احداث ساختمان و تأسیسات پایه دیتاستر): ۱۴ ماه پس از اتمام فاز صفر
- فاز دو (تجهیز فنی، نصب سرورها و سیستم‌های شبکه، تست‌های یکپارچه‌سازی و اخذ گواهینامه‌های بین‌المللی): ۱۰ ماه

پس از اتمام فاز یک

- فاز سه (راه‌اندازی تجاری، جذب مشتریان اولیه و بهره‌برداری پایلوت): ۶ ماه پس از اتمام فاز دو
- فاز چهار (بهره‌برداری کامل، توسعه خدمات ارزش‌افزوده و دستیابی به ظرفیت اسمی): ۱۲ ماه پس از فاز سه
- افق کلان بازگشت سرمایه و سودآوری پایدار: ۶.۵ سال از تاریخ شروع فاز اجرایی
- افق توسعه منطقه‌ای و تبدیل به هاب داده‌ای غرب آسیا: ۱۲ سال از تاریخ تصویب طرح

بخش دوم: تعریف و تشریح طرح

این طرح با هدف ایجاد یک دیتاستر تخصصی، امن و مقیاس‌پذیر در منطقه آزاد شهر فرودگاهی امام خمینی (ره) طراحی شده است که به‌عنوان زیرساخت حیاتی دیجیتال برای اکوسیستم کسب و کارهای منطقه، شرکت‌های بین‌المللی فعال در حوزه تجارت الکترونیک، مؤسسات مالی و بانکی، استارت‌آپ‌های فناوری‌محور و نهادهای حاکمیتی عمل خواهد کرد. دیتاستر پیشنهادی با زیربنای حدود ۴۰۰۰ مترمربع و طراحی مبتنی بر استانداردهای بین‌المللی ANSI/TIA-942-B برای گرید Tier III با قابلیت ارتقای معماری به Tier IV، ظرفیت میزبانی بیش از ۸۰۰ رک سرور، پردازش سالانه بیش از ۵۰ پتابایت داده، و ارائه طیف کاملی از خدمات زیرساختی، پلتفرمی و نرم‌افزاری را دارا خواهد بود.

رکن اول: زیرساخت فیزیکی و تأسیساتی پیشرفته ساختمان دیتاستر با طراحی ماژولار و انعطاف‌پذیر، شامل فضاهای تخصصی ذیل می‌باشد: سالن‌های اصلی میزبانی سرور (White Space) با مساحت حدود ۲۵۰۰ مترمربع و قابلیت پیکربندی پویا بر اساس نیاز مشتریان، اتاق‌های کنترل و عملیات شبکه (NOC) و مرکز عملیات امنیت (SOC) با سیستم‌های مانیتورینگ بلادرنگ، فضاهای پشتیبانی فنی شامل انبار قطعات یدکی، کارگاه تعمیرات و کالیبراسیون تجهیزات، اتاق‌های برق و ژنراتور با سیستم‌های توزیع برق افزونه (Redundant Power Distribution)، سیستم‌های خنک‌کنندگی دقیق با معماری Hot/Cold Aisle Containment برای بهینه‌سازی مصرف انرژی، و فضاهای اداری و خدماتی برای تیم‌های فنی و پشتیبانی. کلیه فضاهای حیاتی با سیستم‌های امنیتی فیزیکی لایه‌ای شامل کنترل دسترسی بیومتریک چندعاملی، دوربین‌های مداربسته هوشمند با تحلیل رفتاری، و گشت‌های امنیتی ۷/۲۴ حفاظت می‌شوند.

رکن دوم: پلتفرم خدمات زیرساختی و ابری (IaaS/PaaS/SaaS) دیتاستر پیشنهادی طیف کاملی از خدمات دیجیتال را در سه لایه ارائه می‌دهد: لایه زیرساخت به‌عنوان سرویس (IaaS) شامل اجاره فضای رک، سرورهای اختصاصی و اشتراکی، ذخیره‌سازی ابری مقیاس‌پذیر، پهنای باند اختصاصی با تضمین کیفیت سرویس (SLA)، و خدمات پشتیبان‌گیری و بازیابی فاجعه؛ لایه پلتفرم به‌عنوان سرویس (PaaS) شامل محیط‌های توسعه و تست ابری، سرویس‌های کانتنری و

اورکسترسیون (Kubernetes)، پایگاه‌های داده مدیریت‌شده، و ابزارهای هوش مصنوعی و تحلیل داده؛ و لایه نرم‌افزار به‌عنوان سرویس (SaaS) شامل ارائه نرم‌افزارهای تخصصی صنعتی، پلتفرم‌های مدیریت کسب‌وکار، و راه‌حل‌های امنیتی ابری. تمامی خدمات با قراردادهای سطح سرویس (SLA) شفاف با تضمین دسترسی‌پذیری ۹۹.۹۸۲٪ برای گرید Tier III و ۹۹.۹۹۵٪ برای حالت ارتقایافته Tier IV ارائه می‌گردند.

رکن سوم: مرکز تخصصی امنیت سایبری و انطباق مقرراتی با توجه به حساسیت داده‌های میزبانی‌شده، دیتاستر شامل یک مرکز عملیات امنیت (SOC) پیشرفته با قابلیت‌های ذیل می‌باشد: پایش بلادرنگ ترافیک شبکه و شناسایی ناهنجاری‌ها با استفاده از هوش مصنوعی و یادگیری ماشین، سیستم‌های تشخیص و پیشگیری از نفوذ لایه‌ای (IDS/IPS)، مدیریت یکپارچه هویت و دسترسی (IAM) با پشتیبانی از احراز هویت چندعاملی، مرکز پاسخ به حوادث سایبری (CSIRT) با تیم‌های واکنش سریع ۷/۲۴، و واحد تخصصی انطباق مقرراتی برای اطمینان از رعایت استانداردهای بین‌المللی حفاظت از داده مانند اصول مشابه GDPR، مقررات مالی (PCI-DSS)، و دستورالعمل‌های حاکمیتی ایران. این مرکز همچنین خدمات ممیزی امنیتی، تست نفوذ، و مشاوره انطباق را به مشتریان ارائه می‌دهد.

رکن چهارم: اکوسیستم نوآوری و همکاری‌های استراتژیک دیتاستر به‌عنوان هسته اکوسیستم دیجیتال منطقه، با ایجاد فضاهای کار اشتراکی برای استارت‌آپ‌های فناوری‌محور، راه‌اندازی آزمایشگاه‌های تست و توسعه برای شرکت‌های نرم‌افزاری، و تسهیل همکاری‌های پژوهشی با دانشگاه‌ها و مراکز تحقیقاتی، بستری برای رشد نوآوری‌های دیجیتال فراهم می‌آورد. همچنین، انعقاد تفاهم‌نامه‌های همکاری با دیتاسترهای بین‌المللی معتبر برای ارائه خدمات میزبانی ترکیبی (Hybrid Cloud)، تبادل ترافیک داده (Peering)، و پشتیبانی از مشتریان چندملیتی، جایگاه منطقه آزاد شهر فرودگاهی را به‌عنوان دروازه دیجیتال ایران به بازارهای منطقه‌ای و بین‌المللی تقویت می‌نماید.

کل طرح بر پایه اصول «پایداری محیط‌زیستی»، «حاکمیت داده»، «انطباق قانونی کامل» و «تعالی عملیاتی» استوار است و تمامی فعالیت‌ها در چارچوب قوانین مناطق آزاد تجاری-صنعتی ایران، قانون تجارت الکترونیک، آیین‌نامه‌های سازمان تنظیم مقررات و ارتباطات رادیویی، و استانداردهای بین‌المللی فناوری اطلاعات انجام خواهد پذیرفت.

بخش سوم: هدف طرح در سه سطح کلان، میانی و خرد

الف) اهداف کلان (سطح استراتژیک):

۱. تبدیل منطقه آزاد شهر فرودگاهی امام خمینی (ره) به قطب منطقه‌ای زیرساخت‌های دیجیتال و خدمات ابری در غرب آسیا
۲. با الهام از مدل‌های موفق دبی، سنگاپور و فرانکفورت ایجاد زیرساخت حیاتی و امن برای میزبانی داده‌های حساس کسب‌وکارهای داخلی و بین‌المللی با رعایت کامل الزامات حاکمیتی، امنیتی و حریم خصوصی داده‌ها
۳. جذب سرمایه‌گذاری مستقیم خارجی در حوزه فناوری اطلاعات و خدمات دیجیتال از طریق ارائه بسته‌های تشویقی منطبق با قوانین مناطق آزاد و مقررات بین‌المللی سرمایه‌گذاری
۴. توسعه صادرات خدمات زیرساختی و ابری ایران به بازارهای منطقه‌ای (عراق، افغانستان، کشورهای

CIS، خلیج فارس) با ایجاد مزیت رقابتی مبتنی بر کیفیت، قیمت و انطباق قانونی ۵. تقویت حاکمیت دیجیتال و استقلال فناوریانه کشور از طریق بومی سازی و توسعه راه حل های زیرساختی پیشرفته در چارچوب استانداردهای جهانی

ب) اهداف میانی (سطح عملیاتی):

۱. راه اندازی دیتاستر با ظرفیت اولیه ۴۰۰ رک سرور در سال اول بهره برداری و دستیابی به ظرفیت کامل ۸۰۰ رک در پایان سال سوم ۲. جذب حداقل ۵۰ مشتری استراتژیک شامل شرکت های بین المللی، مؤسسات مالی، استارت آپ های فناوری محور و نهادهای حاکمیتی در سه سال اول عملیات ۳. دستیابی به شاخص دسترسی پذیری (Uptime) حداقل ۹۹.۹۸۲٪ مطابق با استاندارد Tier III و اخذ گواهینامه های بین المللی ISO 27001, ISO 20000, PCI-DSS تا پایان فاز دو ۴. کاهش مصرف انرژی ویژه (PUE) دیتاستر به کمتر از ۱.۴ در سال سوم بهره برداری از طریق به کارگیری فناوری های خنک کنندگی پیشرفته و مدیریت هوشمند مصرف ۵. ایجاد اشتغال مستقیم برای حداقل ۱۲۰ نفر نیروی انسانی متخصص در حوزه های فنی، امنیتی و مدیریتی و اشتغال غیرمستقیم برای بیش از ۴۰۰ نفر در اکوسیستم دیجیتال منطقه

ج) اهداف خرد (سطح تاکتیکی و فنی): ۱. طراحی و پیاده سازی معماری شبکه دیتاستر با پهنای باند هسته ۱۰۰ گیگابیت بر ثانیه، افزونگی کامل مسیرهای ارتباطی، و مکانیزم های تعادل بار هوشمند ۲. استقرار سیستم مدیریت زیرساخت دیتاستر (DCIM) یکپارچه برای پایش بلادرنگ دما، رطوبت، مصرف برق، ظرفیت سرورها و تولید گزارش های تحلیلی بهینه سازی ۳. پیاده سازی چارچوب امنیت سایبری لایه ای شامل دیوارهای آتش نسل جدید، سیستم های تشخیص نفوذ مبتنی بر هوش مصنوعی، و پروتکل های رمزنگاری پیشرفته برای داده های در حال انتقال و ذخیره شده ۴. طراحی مکانیزم های پشتیبان گیری خودکار با فرکانس ساعتی، تکرار داده بلادرنگ به سایت جغرافیایی مجزا، و قابلیت بازیابی فاجعه با RPO کمتر از ۱۵ دقیقه و RTO کمتر از ۱ ساعت ۵. استقرار فرآیندهای مدیریت خدمت مبتنی بر ITIL 4 برای تضمین کیفیت خدمات، مدیریت تغییرات، و پاسخگویی سریع به درخواست ها و حوادث مشتریان

بخش چهارم: ضرورت، مزایا و فرصت های ایجاد شده طرح

ضرورت اجرای طرح:

۱. ضرورت پاسخگویی به رشد انفجاری تقاضا برای زیرساخت های دیجیتال در ایران و منطقه: با گسترش کسب و کارهای دیجیتال، بانکداری الکترونیک، دولت الکترونیک و اینترنت اشیا، تقاضا برای خدمات دیتاستری امن و مقیاس پذیر به شدت در حال افزایش است و ظرفیت های موجود پاسخگوی این نیاز فزاینده نیستند. ۲. ضرورت بهره گیری از مزیت های استراتژیک منطقه آزاد شهر فرودگاهی: موقعیت جغرافیایی ممتاز در مجاورت فرودگاه بین المللی امام خمینی، دسترسی به فیبر نوری بین المللی، معافیت های قانونی مناطق آزاد، و نزدیکی به مراکز کسب و کار تهران، این منطقه را به کاندیدای ایده آلی برای استقرار دیتاستر منطقه ای تبدیل کرده است. ۳. ضرورت حاکمیت داده و امنیت سایبری در شرایط ژئوپلیتیک پیچیده: با توجه به حساسیت داده های ملی و تجاری و افزایش تهدیدات سایبری، ایجاد زیرساخت های میزبانی داده بومی با استانداردهای امنیتی بین المللی نه تنها یک فرصت اقتصادی، بلکه یک ضرورت استراتژیک برای حفظ حاکمیت دیجیتال کشور محسوب می شود. ۴. ضرورت همگامی با

تحولات جهانی فناوری ابری و لبه (Edge Computing): رشد سریع محاسبات ابری، لبه و ترکیبی (Hybrid/Multi-Cloud) در سطح جهانی، نیازمند پاسخ هوشمندانه اکوسیستم فناوری ایران است تا از قافله تحولات عقب نماند و بتواند سهم خود از بازارهای نوظهور را کسب نماید. ۵. ضرورت ایجاد اکوسیستم یکپارچه نوآوری دیجیتال: پراکندگی فعلی مراکز داده، نبود استانداردهای یکپارچه خدمات، و عدم دسترسی کسب و کارهای کوچک و متوسط به زیرساخت‌های پیشرفته ابری، از موانع اصلی رشد اقتصاد دیجیتال کشور است. این طرح با ایجاد یک دیتاستر مرجع، این خلأها را پوشش می‌دهد.

مزایای مستقیم طرح: ۱. ایجاد اشتغال مستقیم و باکیفیت برای بیش از ۱۲۰ نفر نیروی انسانی متخصص در حوزه‌های مهندسی شبکه، امنیت سایبری، مدیریت دیتاستر و خدمات فنی با حقوق و مزایای رقابتی بین‌المللی ۲. جذب سرمایه‌گذاری مستقیم خارجی به میزان حداقل ۸۰ میلیون یورو در افق ده‌ساله از طریق جذب شرکت‌های بین‌المللی فناوری اطلاعات و ارائه‌دهندگان خدمات ابری منطقه‌ای ۳. افزایش درآمدهای ارزی منطقه آزاد از طریق ارائه خدمات زیرساختی و ابری به مشتریان داخلی و بین‌المللی، اخذ حق اشتراک و کارمزد خدمات، و دریافت سهم از سود همکاری‌های استراتژیک ۴. کاهش هزینه‌های زیرساخت دیجیتال برای کسب و کارهای ایرانی از طریق ارائه خدمات مقیاس‌پذیر با مدل پرداخت بر اساس مصرف (Pay-as-you-go)، حذف نیاز به سرمایه‌گذاری سنگین اولیه در سخت‌افزار، و بهره‌مندی از تخصص فنی مرکز ۵. توسعه صادرات خدمات فنی-مهندسی و مشاوره‌ای در حوزه مدیریت دیتاستر و امنیت سایبری به کشورهای همسایه از طریق مرکز تخصصی طرح

مزایای غیرمستقیم و فرصت‌های ایجاد شده: ۱. تقویت برند و اعتبار بین‌المللی ایران در حوزه زیرساخت‌های دیجیتال پیشرفته و ایجاد تصویر «مرکز داده قابل اعتماد منطقه‌ای» که می‌تواند زمینه‌ساز جذب پروژه‌های بزرگتر و همکاری‌های استراتژیک شود ۲. توسعه دانش بومی و ایجاد مالکیت فکری در حوزه‌های حساس مدیریت داده، بهینه‌سازی مصرف انرژی و امنیت سایبری که می‌تواند به عنوان دارایی استراتژیک کشور در مذاکرات بین‌المللی مورد استفاده قرار گیرد ۳. ایجاد اثرات سرریز (Spillover Effects) بر سایر بخش‌های اقتصادی از طریق تسهیل دیجیتال‌سازی فرآیندها، افزایش بهره‌وری بنگاه‌ها، و توانمندسازی استارت‌آپ‌ها برای رشد و رقابت در بازارهای جهانی ۴. تقویت همکاری‌های منطقه‌ای و بین‌المللی از طریق ایجاد پلتفرمی برای تعامل ارائه‌دهندگان خدمات دیجیتال، مشتریان و نهادهای نظارتی کشورهای مختلف در چارچوبی شفاف و استاندارد ۵. آماده‌سازی زیرساخت‌های فنی، انسانی و حقوقی برای بهره‌برداری از فرصت‌های نوظهور فناوری‌های دیجیتال جهانی مانند اینترنت اشیا صنعتی (IIoT)، شهر هوشمند، و محاسبات کوانتومی در چارچوب مقررات ملی

بخش پنجم: نمونه‌های مشابه جهانی به همراه رفرنس دقیق و جمع‌بندی درس‌های کلیدی

نمونه اول: دیتاسترهای منطقه آزاد دبی Dubai Internet City و Dubai Silicon Oasis منطقه آزاد دبی سلیکون اوئیس با راه‌اندازی دیتاسترهای گرید Tier III و IV و ارائه خدمات ابری به شرکت‌های منطقه MENA، توانسته است بیش از ۱,۲۰۰ شرکت فناوری را جذب کند و حجم سرمایه‌گذاری بخش فناوری اطلاعات را به بیش از ۳ میلیارد دلار

برسانند. درس کلیدی: ترکیب معافیت‌های مالیاتی مناطق آزاد با زیرساخت‌های دیجیتال پیشرفته و چارچوب قانونی شفاف، جذابیت بالایی برای سرمایه‌گذاران بین‌المللی ایجاد می‌کند.

نمونه دوم: دیتاسترهای فرودگاهی اروپا (فرودگاه فرانکفورت و آمستردام اسخیپهول) فرودگاه فرانکفورت

به‌عنوان یکی از بزرگترین هاب‌های داده اروپا، با بهره‌گیری از مزیت اتصال مستقیم به شبکه‌های فیبر نوری بین‌قاره‌ای و نزدیکی به مراکز مالی، دیتاسترهایی با تراکم بالا و تاخیر کم (Low-Latency) برای مؤسسات مالی و تجارت الکترونیک ایجاد کرده است. درس کلیدی: تلفیق مزیت لجستیکی فرودگاه با نیازهای کسب‌وکارهای دیجیتال حساس به تاخیر، ارزش افزوده قابل توجهی ایجاد می‌کند و تمایز رقابتی پایدار ایجاد می‌نماید.

نمونه سوم: دیتاسترهای سبز سنگاپور (سنگاپور به‌عنوان پیشرو در دیتاسترهای پایدار) سنگاپور با اعمال

استانداردهای سختگیرانه مصرف انرژی (حداکثر PUE مجاز ۱.۳) و ارائه مشوق‌های مالی برای دیتاسترهای سبز، توانسته است همزمان با رشد صنعت داده، مصرف انرژی و کربن را کنترل کند. شرکت‌هایی مانند Equinix و Digital Realty در سنگاپور از سیستم‌های خنک‌کنندگی با آب دریا و انرژی خورشیدی استفاده می‌کنند. درس کلیدی: در شرایط محدودیت‌های محیط‌زیستی و انرژی، طراحی دیتاستر با رویکرد پایداری نه تنها یک الزام قانونی، بلکه یک مزیت رقابتی و جذابیت برای مشتریان مسئولیت‌پذیر است.

نمونه چهارم: دیتاسترهای منطقه‌ای ترکیه (استانبول و آنکارا) ترکیه با سرمایه‌گذاری در دیتاسترهای گرید بالا در

مناطق آزاد و ویژه اقتصادی، توانسته است به هاب داده‌ای برای ترافیک بین اروپا، خاورمیانه و آسیای مرکزی تبدیل شود. موقعیت جغرافیایی، هزینه‌های عملیاتی نسبتاً پایین، و چارچوب قانونی نسبتاً منعطف، عوامل کلیدی موفقیت این مدل بوده‌اند. درس کلیدی: موقعیت ژئواستراتژیک همراه با هزینه‌های رقابتی و چارچوب قانونی شفاف، می‌تواند دیتاستر یک کشور در حال توسعه را به نقطه اتصال ترافیک داده منطقه‌ای تبدیل کند.

جمع‌بندی درس‌های کلیدی برای طرح پیشنهادی در منطقه آزاد شهر فرودگاهی امام خمینی (ره):

۱. ضرورت طراحی دیتاستر با استانداردهای بین‌المللی (Tier III/IV, ISO 27001, PCI-DSS) از همان ابتدا برای جلب اعتماد مشتریان بین‌المللی و امکان رقابت در بازار منطقه‌ای.
۲. اهمیت تلفیق مزیت‌های جغرافیایی و لجستیکی فرودگاه امام خمینی با نیازهای کسب‌وکارهای دیجیتال حساس به تاخیر و پهنای باند برای ایجاد ارزش منحصربه‌فرد.
۳. نیازمند طراحی زیرساخت با رویکرد پایداری محیط‌زیستی PUE هدف کمتر از ۱.۴، استفاده از انرژی‌های تجدیدپذیر، مدیریت هوشمند آب، برای انطباق با استانداردهای جهانی و کاهش هزینه‌های بلندمدت عملیاتی.
۴. ضرورت ایجاد چارچوب قانونی و نظارتی شفاف برای میزبانی داده‌های حساس با هماهنگی کامل با نهادهای حاکمیتی ملی (سازمان تنظیم مقررات، مرکز افتا، بانک مرکزی) و رعایت اصول حاکمیت داده.
۵. اهمیت ایجاد شبکه‌ای از شرکای استراتژیک بین‌المللی (ارائه‌دهندگان ابری جهانی، اپراتورهای فیبر نوری، مراکز تحقیقاتی) برای تسریع انتقال فناوری، افزایش اعتبار و دسترسی به بازارهای هدف.

بخش ششم: موقعیت مکانی طرح با تحلیل چندلایه

لایه اول: تحلیل جغرافیایی-استراتژیک منطقه آزاد شهر فرودگاهی امام خمینی (ره) در موقعیت استثنایی واقع در ۳۰

کیلومتری جنوب غربی تهران و در مجاورت مستقیم فرودگاه بین‌المللی امام خمینی قرار دارد. این موقعیت جغرافیایی برای استقرار دیتاسنتر تخصصی دارای مزایای استراتژیک چندبعدی است: اولاً، دسترسی مستقیم به کابل‌های فیبر نوری بین‌المللی که از مسیر فرودگاه عبور می‌کنند، امکان اتصال با تاخیر کم (Low-Latency) به شبکه‌های داده اروپا، آسیا و خاورمیانه را فراهم می‌آورد که برای خدمات ابری، معاملات مالی الکترونیکی و پلتفرم‌های تجارت الکترونیک حیاتی است. ثانیاً، فاصله بهینه از مرکز کلان‌شهر تهران (کاهش ریسک‌های امنیتی شهری، آلودگی و ترافیک) همراه با دسترسی آسان به مراکز علمی، پژوهشی و نیروی انسانی متخصص پایتخت، تعادلی استراتژیک بین امنیت عملیاتی و دسترسی به منابع انسانی نخبه ایجاد نموده است. ثالثاً، هم‌جواری با فرودگاه بین‌المللی به عنوان بزرگترین دروازه هوایی کشور، امکان ارائه خدمات دیتاسنتری با تاخیر فوق‌العاده کم به شرکت‌های هواپیمایی، لجستیک دیجیتال و مسافران بین‌المللی را ایجاد می‌کند که یک مزیت رقابتی منحصر به فرد در منطقه محسوب می‌شود.

لایه دوم: تحلیل زیرساختی-فنی منطقه مورد نظر از نظر زیرساخت‌های فنی مورد نیاز دیتاسنتر دارای شرایط ممتازی

است: شبکه برق با پایداری بالا و امکان تأمین برق اضطراری از طریق ژنراتورهای دیزلی صنعتی با ظرفیت کافی برای حداقل ۷۲ ساعت کارکرد مستقل، همراه با سیستم‌های UPS صنعتی با زمان سوئیچ زیر ۱۰ میلی ثانیه برای تضمین تداوم برق بدون وقفه (Zero Downtime) برای سرورها و تجهیزات حیاتی. شبکه فیبر نوری با پهنای باند اختصاصی و امکان اتصال به شبکه‌های بین‌المللی اینترنت از طریق دروازه‌های مخابراتی مجاز سازمان تنظیم مقررات و ارتباطات رادیویی، با پشتیبانی از پروتکل‌های BGP برای مسیریابی پویا و افزونگی مسیرها. سیستم آب‌رسانی صنعتی با ظرفیت کافی برای سیستم‌های خنک‌کنندگی تبخیری و برج‌های خنک‌کننده، همراه با شبکه فاضلاب و تصفیه‌خانه اختصاصی برای مدیریت پساب‌های صنعتی. سیستم اطفاء حریق پیشرفته مطابق با استانداردهای NFPA 75 و ۲۰۰۱ با استفاده از گازهای پاک Novec 1230 یا FM200 که برای فضاهای حساس الکترونیکی بدون باقیمانده مخرب عمل می‌کنند. سیستم امنیت فیزیکی لایه‌ای شامل کنترل دسترسی بیومتریک چندعاملی (اثر انگشت، تشخیص چهره، کارت هوشمند)، دوربین‌های مدار بسته هوشمند با تحلیل تصویر و تشخیص رفتار مشکوک، و گشت‌های امنیتی تخصصی آموزش دیده برای دیتاسنتر. علاوه بر این، وجود زیرساخت‌های ارتباطی رادیویی و ماهواره‌ای پشتیبان، امکان تنوع بخشی به مسیرهای ارتباطی و افزایش تاب‌آوری شبکه را فراهم می‌آورد.

لایه سوم: تحلیل قانونی-حکمرانی منطقه آزاد شهر فرودگاهی امام خمینی (ره) تحت حاکمیت قانون چگونگی اداره

مناطق آزاد تجاری-صنعتی جمهوری اسلامی ایران مصوب ۱۳۷۲ و اصلاحات بعدی آن اداره می‌شود. این چارچوب قانونی مزایای قابل توجهی برای طرح دیتاسنتر ایجاد می‌کند: معافیت مالیاتی ۲۰ ساله برای فعالیت‌های تولیدی و خدماتی فناوری اطلاعات، معافیت از حقوق گمرکی برای واردات ماشین‌آلات، تجهیزات تخصصی دیتاسنتر و قطعات یدکی مورد نیاز، امکان جذب سرمایه‌گذاری خارجی با تضمین‌های قانونی مطابق قانون تشویق و حمایت سرمایه‌گذاری خارجی مصوب ۱۳۸۰، استقلال نسبی در تعیین مقررات داخلی منطقه با تأیید شورای عالی مناطق آزاد در حوزه‌های فنی و خدماتی، و امکان انعقاد قراردادهای

بین‌المللی با اشخاص حقوقی خارجی برای ارائه خدمات فرامرزی. علاوه بر این، آیین‌نامه عملیات پولی و بانکی در مناطق آزاد امکان افتتاح حساب‌های ارزی، دریافت و پرداخت‌های بین‌المللی و ارائه خدمات مالی ویژه به مشتریان خارجی را در چارچوب مقررات بانک مرکزی فراهم می‌آورد. همچنین، هماهنگی با سازمان تنظیم مقررات و ارتباطات رادیویی برای اخذ مجوزهای ارائه خدمات ارتباطی و داده‌ای، و با مرکز افتا برای رعایت الزامات امنیت سایبری حاکمیتی، چارچوب قانونی جامعی برای فعالیت دیتاسنتر ایجاد می‌نماید.

لایه چهارم: تحلیل اکوسیستمی-هم‌افزایی موقعیت طرح در مجاورت شهرک‌های صنعتی استان تهران (شهرک صنعتی شمس‌آباد، شهرک صنعتی چهاردانگه، شهرک صنعتی پرند) و مناطق آزاد و ویژه اقتصادی همجوار امکان ایجاد هم‌افزایی و زنجیره ارزش تکمیلی را فراهم می‌کند. شرکت‌های مستقر در شهرک‌های صنعتی می‌توانند از خدمات میزبانی، ابر و امنیت سایبری دیتاسنتر برای دیجیتال‌سازی فرآیندهای تولید، مدیریت زنجیره تأمین و تجارت الکترونیک استفاده نمایند و در مقابل، دیتاسنتر می‌تواند با درک نیازهای واقعی صنعت، خدمات خود را بهینه‌سازی و تخصصی‌تر نماید. همچنین، همکاری با مراکز پژوهشی و دانشگاهی تهران (دانشگاه صنعتی شریف، دانشگاه تهران، پژوهشگاه ارتباطات و فناوری اطلاعات، دانشگاه علم و صنعت) امکان دسترسی به نیروی انسانی نخبه، همکاری‌های پژوهشی مشترک در حوزه‌های بهینه‌سازی مصرف انرژی دیتاسنتر، امنیت سایبری پیشرفته و هوش مصنوعی، و انتقال فناوری‌های نوین را تسهیل می‌نماید. علاوه بر این، هم‌افزایی با طرح مرکز اقتصاد دیجیتال و فین‌تک منطقه، امکان ارائه خدمات ترکیبی زیرساختی-مالی به استارت‌آپ‌ها و مؤسسات مالی را ایجاد می‌کند که ارزش افزوده قابل توجهی برای هر دو طرح دارد.

لایه پنجم: تحلیل اقلیمی-محیط‌زیستی اقلیم نیمه‌خشک منطقه تهران با میانگین دمای سالانه ۱۷ درجه سانتی‌گراد، روزهای آفتابی زیاد (بیش از ۳۰۰ روز در سال) و رطوبت نسبی متوسط، شرایط مناسبی برای استقرار دیتاسنتر با سیستم‌های خنک‌کنندگی ترکیبی فراهم می‌کند. با بهره‌گیری از سیستم‌های خنک‌کنندگی طبیعی (Free Cooling) در فصول خنک سال، استفاده از تبخیر غیرمستقیم (Indirect Evaporative Cooling) در فصول گرم، و نصب پنل‌های خورشیدی برای تأمین بخشی از برق مورد نیاز، می‌توان شاخص مصرف انرژی (PUE) دیتاسنتر را به کمتر از ۱.۴ رساند که مطابق با استانداردهای دیتاسنترهای سبز جهانی است. با این حال، طرح باید تمهیدات لازم برای مدیریت مصرف آب (با توجه به محدودیت‌های آبی منطقه تهران) از طریق سیستم‌های بازیافت و چرخش آب خنک‌کننده، کاهش انتشار کربن از طریق استفاده از انرژی‌های تجدیدپذیر و خرید گواهی کربن، مدیریت پسماندهای الکترونیکی مطابق با استانداردهای زیست‌محیطی WEEE، و رعایت اصول ساختمان‌سازی سبز گرید LEED یا BREEAM را در طراحی و اجرا مدنظر قرار دهد. همچنین، انجام ارزیابی اثرات زیست‌محیطی (EIA) پیش از شروع عملیات اجرایی و تدوین برنامه مدیریت زیست‌محیطی (EMP) برای پایش و کاهش اثرات منفی طرح، از الزامات قانونی و اخلاقی پروژه محسوب می‌شود.

لایه ششم: تحلیل ریسک-امنیتی موقعیت مکانی طرح از نظر امنیتی دارای نقاط قوت و چالش‌هایی است: از یک سو، قرارگیری در محدوده تحت حفاظت فرودگاه بین‌المللی و وجود نیروهای امنیتی تخصصی هوانوردی، سطح بالایی از امنیت فیزیکی در برابر تهدیدات خارجی را تضمین می‌کند. از سوی دیگر، حساسیت داده‌های میزبانی‌شده در دیتاسنتر و ارزش

استراتژیک زیرساخت دیجیتال، نیازمند تدابیر امنیتی سایبری پیشرفته شامل دیوارهای آتش لایه‌ای با بازرسی عمیق بسته‌ها (Deep Packet Inspection)، سیستم‌های تشخیص و پیشگیری از نفوذ مبتنی بر هوش مصنوعی (AI-based IDS/IPS)، مرکز عملیات امنیت (SOC) با پیش ۷/۲۴ و تیم پاسخ به حوادث سایبری (CSIRT) آماده‌باش، و پروتکل‌های رمزنگاری پیشرفته برای داده‌های در حال انتقال و ذخیره‌شده است. همچنین، تنوع بخشی به مسیرهای ارتباطی اینترنت (از طریق اپراتورهای مختلف داخلی، لینک‌های فیبر نوری بین‌المللی و ارتباطات ماهواره‌ای پشتیبان) و استقرار سیستم‌های بک‌آپ و بازیابی فاجعه (Disaster Recovery) در سایت‌های جغرافیایی مجزا با فاصله حداقل ۱۰۰ کیلومتر، از الزامات حیاتی برای تضمین تداوم کسب‌وکار و تاب‌آوری در برابر حوادث طبیعی یا انسان‌ساخت محسوب می‌شود. علاوه بر این، طراحی ساختمان دیتاستر با رعایت استانداردهای مقاومت در برابر زلزله (تا شدت ۸ ریشتر مطابق آیین‌نامه ۲۸۰۰ ایران)، سیل، و حوادث غیرمترقبه، و استقرار سیستم‌های اطفاء حریق گازی بدون آسیب به تجهیزات الکترونیکی، از ملاحظات ایمنی حیاتی طرح است.

بخش هفتم: پیشیازها و زیرساخت‌های لازم طرح با تحلیل جامع

الف) زیرساخت‌های قانونی و حکمرانی:

۱. اخذ مجوز فعالیت دیتاستر از سازمان مناطق آزاد تجاری-صنعتی ایران مطابق با ضوابط و مقررات حاکم بر مناطق آزاد و با تأکید بر انطباق خدمات داده‌ای و ابری با سیاست‌های کلی نظام و مقررات سازمان تنظیم مقررات و ارتباطات رادیویی. ۲. اخذ مجوز ارائه خدمات ارتباطی و داده‌ای از سازمان تنظیم مقررات و ارتباطات رادیویی (رگولاتوری) شامل مجوز مرکز داده، مجوز ارائه خدمات ابری، و مجوز اتصال به شبکه بین‌الملل، با رعایت شرایط فنی و امنیتی تعیین شده. ۳. اخذ تأییدیه امنیتی از مرکز افتای ریاست جمهوری برای میزبانی داده‌های حساس و ارائه خدمات به نهادهای حاکمیتی، شامل رعایت الزامات امنیتی سخت‌افزاری، نرم‌افزاری و فرآیندی تعیین شده در اسناد بالادستی امنیت فضای تولید و تبادل اطلاعات کشور. ۴. تدوین و تصویب «نظام‌نامه داخلی خدمات دیتاستر و ابری» در منطقه آزاد شهر فرودگاهی با مشارکت کارشناسان فنی، حقوقی و امنیتی و با تأیید شورای عالی مناطق آزاد و نهادهای ذی‌ربط ملی، شامل مقررات سطح سرویس (SLA)، سیاست‌های حفظ حریم خصوصی داده، و چارچوب‌های پاسخ به حوادث. ۵. ایجاد «کمیته نظارت فنی و امنیتی دیتاستر» متشکل از نمایندگان سازمان مناطق آزاد، سازمان تنظیم مقررات، مرکز افتا، و کارشناسان مستقل برای نظارت مستمر بر عملکرد فنی، امنیتی و انطباقی دیتاستر و اطمینان از رعایت استانداردهای الزامی. ۶. طراحی و استقرار سیستم حاکمیت شرکتی (Corporate Governance) شفاف برای بهره‌برداری از دیتاستر شامل اساسنامه، آیین‌نامه‌های داخلی، کمیته‌های تخصصی (فنی، امنیت، ریسک، حسابرسی) و مکانیزم‌های گزارش‌دهی به سرمایه‌گذاران و نهادهای نظارتی.

ب) زیرساخت‌های مالی و تأمین سرمایه:

۱. تأمین سرمایه اولیه ۴۵ میلیون یورویی از طریق ترکیبی از منابع: سهم منطقه آزاد شهر فرودگاهی (۳۵٪)، سرمایه‌گذاران استراتژیک داخلی (۴۰٪)، سرمایه‌گذاران خارجی واجد شرایط (۱۵٪) و تسهیلات بانکی یا صکوک اسلامی سبز ۱۰٪. ۲. ایجاد ساختار حقوقی بهینه برای بهره‌برداری از دیتاستر با در نظرگیری قوانین ایران و استانداردهای بین‌المللی، شامل امکان جذب سرمایه

به صورت سهام ممتاز، اوراق مشارکت پروژه محور، یا قراردادهای مشارکت مدنی با تقسیم سود و ریسک شفاف. ۳. طراحی مکانیزم های بازگشت سرمایه برای سرمایه گذاران شامل مدل های درآمدی متنوع (اجاره فضای رک، خدمات ابری، پهنای باند، خدمات ارزش افزوده امنیتی)، قراردادهای بلندمدت با مشتریان استراتژیک (Anchor Tenants)، و امکان عرضه سهام شرکت بهره بردار در بورس منطقه یا بین المللی در افق میان مدت. ۴. ایجاد خط اعتباری اضطراری (Emergency Credit Line) با بانک های داخلی و بین المللی همکار برای مدیریت نقدینگی در شرایط غیرمترقبه مانند تأخیر در پرداخت مشتریان یا نیاز به سرمایه گذاری فوری در به روز رسانی تجهیزات. ۵. استقرار سیستم مدیریت ریسک مالی یکپارچه شامل شناسایی، اندازه گیری، پایش و کنترل ریسک های بازار (نوسانات نرخ ارز و هزینه انرژی)، اعتباری (تأخیر پرداخت مشتریان)، عملیاتی (خرابی تجهیزات) و نقدینگی با بهره گیری از مدل های کمی پیشرفته و بیمه های تخصصی.

ج) زیرساخت های فیزیکی و کالبدی:

۱. احداث ساختمان تخصصی دیتاسنتر با مساحت زیربنایی حدود ۴۰۰۰ مترمربع در دو طبقه اصلی شامل: سالن های میزبانی سرور (White Space) با مساحت حدود ۲۵۰۰ مترمربع و قابلیت پیکربندی پویا، اتاق های کنترل عملیات شبکه (NOC) و مرکز عملیات امنیت (SOC)، فضاهای تأسیساتی شامل اتاق برق اصلی، ژنراتورخانه، سیستم های خنک کنندگی و تصفیه آب، فضاهای پشتیبانی فنی شامل انبار قطعات یدکی، کارگاه کالیبراسیون و تعمیرات، و فضاهای اداری و خدماتی برای تیم های فنی و پشتیبانی. ۲. طراحی معماری ساختمان با رعایت اصول ماژولاریتی (Modularity) و مقیاس پذیری (Scalability) برای امکان توسعه تدریجی ظرفیت بدون اختلال در عملیات جاری، و انعطاف پذیری (Flexibility) برای تطبیق با نیازهای متغیر فناوری و مشتریان. ۳. تأمین سیستم های تأسیساتی پیشرفته شامل تهویه مطبوع دقیق (Precision Cooling) با معماری Hot/Cold Aisle Containment برای بهینه سازی جریان هوا و کاهش مصرف انرژی تا ۴۰٪، سیستم برق اضطراری با ژنراتورهای دیزلی N+1 با ظرفیت کافی برای حداقل ۷۲ ساعت کارکرد مستقل به همراه بانک باتری های UPS با زمان سوئیچ زیر ۱۰ میلی ثانیه، سیستم اطفاء حریق گازی از نوع Novec ۱۲۳۰ یا FM200 با زمان تخلیه کمتر از ۱۰ ثانیه و بدون باقیمانده مخرب برای تجهیزات الکترونیکی. ۴. ایجاد فضای سبز و محیط کاری بهینه با رعایت استانداردهای رفاهی و بهره وری نیروی انسانی (نور طبیعی کنترل شده، کیفیت هوا با فیلتراسیون HEPA، فضاهای استراحت و تعامل، و ارگونومی محیط کار (برای جذب و حفظ نیروی انسانی متخصص). ۵. پیش بینی پارکینگ کافی، دسترسی های معلولین مطابق با استانداردهای بین المللی، و امکانات حمل و نقل داخلی (شاتل برقی) برای تسهیل تردد کارکنان شیفتی و مراجعان فنی.

د) زیرساخت های دیجیتال و فناوری اطلاعات:

۱. راه اندازی زیرساخت شبکه دیتاسنتر با معماری لایه ای شامل سوئیچ های هسته (Core Switches) با ظرفیت ۱۰۰ گیگابیت بر ثانیه و افزونگی کامل، سوئیچ های توزیع و دسترسی با پشتیبانی از پروتکل های SDN (Software-Defined Networking) برای انعطاف پذیری و مدیریت متمرکز، فایروال های نسل جدید (NGFW) با قابلیت بازرسی عمیق بسته ها (Deep Packet Inspection) و پیشگیری از نفوذ (IPS)، و سیستم های تعادل بار (Load Balancers) برای توزیع هوشمند ترافیک و تضمین دسترسی پذیری بالا. ۲. استقرار پلتفرم مدیریت زیرساخت دیتاسنتر (DCIM) یکپارچه برای پایش

بلادرنگ پارامترهای حیاتی شامل دما، رطوبت، مصرف برق هر رک، ظرفیت سرورها، و وضعیت خنک‌کنندگی، همراه با قابلیت تولید گزارش‌های تحلیلی برای بهینه‌سازی مصرف انرژی و پیش‌بینی نیازهای توسعه. ۳. توسعه پلتفرم خدمات ابری مبتنی بر معماری میکروسرویس (Microservices) با قابلیت ارائه خدمات IaaS، PaaS و SaaS، پشتیبانی از کانتینرها و اورکستراسیون با Kubernetes، و یکپارچه‌سازی با سیستم‌های مدیریت هویت و دسترسی (IAM) برای احراز هویت امن کاربران. ۴. پیاده‌سازی سیستم‌های امنیتی سایبری پیشرفته شامل مدیریت هویت و دسترسی چندعاملی (MFA)، رمزنگاری داده‌ها در حال انتقال با TLS 1.3 و داده‌های ذخیره‌شده با AES-256، سیستم‌های تشخیص ناهنجاری مبتنی بر هوش مصنوعی (Anomaly Detection)، و پلتفرم مدیریت اطلاعات و رویدادهای امنیتی (SIEM) برای همبستگی لاگ‌ها و شناسایی تهدیدات پیچیده. ۵. ایجاد محیط تست و شبیه‌سازی (Sandbox Environment) با قابلیت شبیه‌سازی ترافیک واقعی، حملات سایبری کنترل‌شده، و سناریوهای بازیابی فاجعه برای تست ایمن راه‌حل‌های جدید و آموزش تیم‌های فنی بدون ریسک برای محیط عملیاتی.

ه) زیرساخت‌های نیروی انسانی، دانش و مهارت:

۱. جذب و استخدام تیم مدیریت ارشد با تجربه بین‌المللی در حوزه‌های مدیریت دیتاستر، خدمات ابری و امنیت سایبری، ترجیحاً با ترکیبی از تخصص‌های داخلی (آشنایی با مقررات ایران) و بین‌المللی (آشنایی با بهترین روش‌های جهانی). ۲. طراحی و اجرای برنامه جامع جذب و توسعه استعدادها (Talent Acquisition & Development) شامل همکاری با دانشگاه‌های برتر فنی-مهندسی، برگزاری مسابقات تخصصی امنیت سایبری و مدیریت داده، و ارائه بورسیه‌های تخصصی برای دانشجویان مستعد در حوزه‌های اولویت‌دار. ۳. ایجاد آکادمی آموزش تخصصی دیتاستر و ابر با ارائه دوره‌های گواهینامه‌دار در حوزه‌های فنی (مدیریت سرورهای لینوکس/ویندوز، شبکه‌های پیشرفته سیسکو/جونپر، امنیت سایبری و تست نفوذ)، عملیاتی (مدیریت خدمات مبتنی بر ITIL، مدیریت پروژه با PMP)، و تخصصی دیتاستر مدیریت انرژی دیتاستر، استانداردهای TIA-942 و ISO 27001. ۴. استقرار سیستم مدیریت دانش (Knowledge Management) برای مستندسازی تجربیات، بهترین روش‌ها (Best Practices)، و درس‌های آموخته شده از حوادث و پروژه‌ها، و تسهیل اشتراک‌گذاری دانش درون‌سازمانی از طریق پلتفرم‌های دیجیتال و جلسات منظم تبادل تجربه. ۵. طراحی مکانیزم‌های انگیزشی و حفظ نیروی انسانی نخبه شامل بسته‌های جبران خدمات رقابتی با استانداردهای بین‌المللی، امکان مشارکت در سود پروژه‌های موفق، فرصت‌های توسعه شغلی و آموزش‌های بین‌المللی، و محیط کاری الهام‌بخش با تجهیزات و فناوری‌های روز.

و) زیرساخت‌های تأمین تجهیزات، تکنولوژی و مواد مصرفی:

۱. انعقاد قراردادهای تأمین بلندمدت با تولیدکنندگان معتبر سخت‌افزارهای دیتاستر (سرورهای Dell, HPE, Lenovo؛ تجهیزات شبکه سیسکو، آریستا، جونپر؛ سیستم‌های ذخیره‌سازی NetApp, Pure Storage) با در نظرگیری الزامات پشتیبانی فنی محلی، گارانتی بین‌المللی و امکان به‌روزرسانی تدریجی. ۲. ایجاد مکانیزم‌های واردات تسهیل‌شده تجهیزات تخصصی با استفاده از معافیت‌های گمرکی مناطق آزاد و هماهنگی با سازمان‌های ذی‌ربط برای اخذ مجوزهای لازم ورود تجهیزات حساس فناوری، با رعایت مقررات کنترل صادرات بین‌المللی. ۳. توسعه همکاری‌های فناورانه با شرکت‌های پیشرو جهانی در حوزه‌های

محاسبات ابری، امنیت سایبری و بهینه‌سازی انرژی دیتاستر برای انتقال فناوری، لایسنس نرم‌افزار، و پشتیبانی فنی تخصصی، همراه با تعهدات بومی‌سازی تدریجی دانش فنی. ۴. پیش‌بینی بودجه تحقیق و توسعه (حداقل ۱۰٪ از سرمایه اولیه) برای توسعه راه‌حل‌های بومی بهینه‌سازی مصرف انرژی، امنیت سایبری تطبیقی با تهدیدات منطقه‌ای، و مدیریت هوشمند زیرساخت، همراه با ثبت اختراعات و ایجاد مالکیت فکری استراتژیک. ۵. ایجاد انبار استراتژیک قطعات یدکی حیاتی (ماژول‌های حافظه، دیسک‌های SSD، کارت‌های شبکه، منبع تغذیه) با موجودی کافی برای حداقل ۶ ماه عملیات بدون وقفه، همراه با سیستم مدیریت موجودی هوشمند برای پیش‌بینی نیازها و سفارش‌دهی خودکار.

ز) عوامل محیطی و پایداری:

۱. انجام ارزیابی اثرات زیست‌محیطی (EIA) پیش از شروع عملیات اجرایی و تدوین برنامه مدیریت زیست‌محیطی (EMP) برای پایش و کاهش اثرات منفی طرح شامل مصرف انرژی، آب، تولید پسماند الکترونیکی و انتشار کربن. ۲. به‌کارگیری فناوری‌های سبز در طراحی و بهره‌برداری از دیتاستر شامل سیستم‌های خنک‌کنندگی ترکیبی Free Cooling در فصول خنک، تبخیر غیرمستقیم در فصول گرم، نصب پنل‌های خورشیدی با ظرفیت حداقل ۵۰۰ کیلووات برای تأمین بخشی از برق مورد نیاز، و استفاده از مصالح ساختمانی پایدار با عایق‌بندی حرارتی پیشرفته. ۳. استقرار سیستم مدیریت پسماند الکترونیکی (E-Waste Management) مطابق با استانداردهای بین‌المللی WEEE برای جمع‌آوری، تفکیک و بازیافت ایمن تجهیزات فرسوده از طریق شرکت‌های مجاز، با هدف دستیابی به نرخ بازیافت بالای ۹۰٪. ۴. طراحی برنامه مسئولیت اجتماعی شرکتی (CSR) با تمرکز بر آموزش دیجیتال به جامعه محلی، حمایت از استارت‌آپ‌های فناوری‌محور منطقه، و کاهش شکاف دیجیتال از طریق ارائه خدمات رایگان یا یارانه‌ای به مؤسسات آموزشی و پژوهشی. ۵. پایش مستمر شاخص‌های پایداری مصرف انرژی ویژه PUE، مصرف آب ویژه WUE، انتشار کربن و گزارش‌دهی شفاف به ذی‌نفعان در چارچوب استانداردهای گزارش‌دهی پایداری مانند GRI و انتشار سالانه گزارش پایداری دیتاستر.

بخش هشتم: خدمات پیشنهادی قابل ارائه طرح و تشریح آنها

خدمت اول: میزبانی تخصصی سرور و فضای رک (Colocation Services) این خدمت پایه‌ای دیتاستر، امکان اجاره فضای فیزیکی امن برای استقرار سرورها، تجهیزات شبکه و ذخیره‌سازی مشتریان را فراهم می‌آورد. فرآیند ارائه این خدمت شامل مراحل ذیل است: مشاوره فنی اولیه برای تعیین نیازهای مشتری از نظر فضای رک، برق مورد نیاز (از ۳ کیلووات تا ۲۰ کیلووات برای هر رک)، پهنای باند و الزامات امنیتی؛ امضای قرارداد سطح سرویس (SLA) با تضمین دسترسی‌پذیری ۹۹.۹۸۲٪، زمان پاسخ به حوادث، و جبران خسارت در صورت عدم تحقق تعهدات؛ تحویل فضای رک با دسترسی فیزیکی کنترل‌شده، برق افزونه از دو منبع مستقل، خنک‌کنندگی دقیق، و اتصال به شبکه هسته دیتاستر با پهنای باند اختصاصی؛ و ارائه خدمات ارزش‌افزوده شامل پشتیبانی فنی ۷/۲۴، مانیتورینگ از راه دور تجهیزات، و گزارش‌دهی دوره‌ای عملکرد. این خدمت

برای شرکت‌هایی که ترجیح می‌دهند مالکیت سخت‌افزار خود را حفظ کنند اما از مزایای زیرساخت حرفه‌ای دیتاستر بهره‌مند شوند، ایده‌آل است.

خدمت دوم: زیرساخت به‌عنوان سرویس (Infrastructure as a Service - IaaS) این خدمت ابری، امکان دسترسی به منابع محاسباتی مجازی‌شده شامل سرورهای مجازی (VMs)، ذخیره‌سازی ابری مقیاس‌پذیر، و شبکه‌های مجازی خصوصی (VPC) را به‌صورت خودخدمت و بر اساس تقاضا فراهم می‌آورد. مشتریان می‌توانند از طریق پورتال وب یا API، منابع مورد نیاز خود را در چند دقیقه تأمین کنند، پیکربندی نمایند، و بر اساس مصرف واقعی (Pay-as-you-go) یا رزرو بلندمدت با تخفیف پرداخت نمایند. پلتفرم IaaS از هایپروایزهای صنعتی مانند VMware vSphere یا KVM پشتیبانی می‌کند، امکان ایجاد اسنپ‌شات و بک‌آپ خودکار از ماشین‌های مجازی را فراهم می‌آورد، و با سیستم‌های مدیریت هویت یکپارچه شده تا دسترسی‌ها به‌صورت دقیق کنترل شوند. این خدمت برای استارت‌آپ‌ها، شرکت‌های در حال رشد، و پروژه‌های موقتی که نیاز به انعطاف و مقیاس‌پذیری بالا دارند، بسیار مناسب است.

خدمت سوم: پلتفرم به‌عنوان سرویس (Platform as a Service - PaaS) این خدمت سطح بالاتر، محیط‌های توسعه، تست و استقرار نرم‌افزار را بدون نیاز به مدیریت زیرساخت پایه ارائه می‌دهد. پلتفرم PaaS شامل سرویس‌های کانتینری با پشتیبانی از Docker و Kubernetes برای اورکستراسیون، پایگاه‌های داده مدیریت‌شده (MySQL, PostgreSQL)، سرویس‌های صف پیام (Message Queues)، و ابزارهای CI/CD برای اتوماسیون فرآیند توسعه نرم‌افزار است. توسعه‌دهندگان می‌توانند کد خود را مستقیماً در پلتفرم استقرار دهند و سیستم به‌صورت خودکار مقیاس‌دهی، بارگذاری و پایش را انجام دهد. این خدمت سرعت توسعه و عرضه محصولات نرم‌افزاری را افزایش داده و نیاز به تخصص عمیق در مدیریت زیرساخت را کاهش می‌دهد، که برای تیم‌های توسعه چابک و شرکت‌های فناوری محور بسیار ارزشمند است.

خدمت چهارم: امنیت سایبری به‌عنوان سرویس (Security as a Service - SECaaS) با توجه به افزایش تهدیدات سایبری، این خدمت طیف کاملی از راه‌حل‌های امنیتی ابری را ارائه می‌دهد: دیوار آتش ابری (Cloud Firewall) با قابلیت فیلترینگ ترافیک ورودی و خروجی بر اساس سیاست‌های تعریف‌شده، سیستم تشخیص و پیشگیری از نفوذ ابری (Cloud IDS/IPS) با به‌روزرسانی بلادرنگ امضای تهدیدات، سرویس مدیریت آسیب‌پذیری و اسکن امنیتی دوره‌ای برنامه‌ها و زیرساخت‌ها، سرویس مدیریت هویت و دسترسی ابری (Cloud IAM) با پشتیبانی از احراز هویت چندعاملی و تک‌ورود (SSO)، و سرویس رمزنگاری و مدیریت کلید ابری برای حفاظت از داده‌های حساس. تمامی این خدمات از طریق پورتال متمرکز قابل مدیریت هستند و گزارش‌های تحلیلی از وضعیت امنیتی ارائه می‌دهند. این خدمت به ویژه برای کسب‌وکارهای کوچک و متوسط که توانایی سرمایه‌گذاری در تیم و ابزارهای امنیتی تخصصی را ندارند، دسترسی به امنیت سطح سازمانی را فراهم می‌آورد.

خدمت پنجم: پشتیبان‌گیری و بازیابی فاجعه به‌عنوان سرویس (Backup & Disaster Recovery as a Service) این خدمت حیاتی، امکان بک‌آپ خودکار و منظم از داده‌ها، برنامه‌ها و سیستم‌های مشتریان را با فرکانس قابل تنظیم

(ساعتی، روزانه، هفتگی) فراهم می‌آورد. داده‌های پشتیبان در سایت جغرافیایی مجزا با فاصله حداقل ۱۰۰ کیلومتر از دیتاستر اصلی ذخیره می‌شوند تا در برابر حوادث محلی (زلزله، سیل، قطع برق گسترده) محافظت شوند. سرویس بازیابی فاجعه (DR) امکان راه‌اندازی سریع محیط عملیاتی جایگزین در سایت پشتیبان با زمان بازیابی (RTO) کمتر از ۱ ساعت و نقطه بازیابی (RPO) کمتر از ۱۵ دقیقه را فراهم می‌آورد. مشتریان می‌توانند سناریوهای بازیابی را به صورت دوره‌ای تست کنند تا از آمادگی سیستم اطمینان حاصل نمایند. این خدمت برای مؤسسات مالی، مراکز درمانی، و هر کسب و کاری که تداوم عملیات برای آن حیاتی است، ضروری است.

خدمت ششم: خدمات تخصصی شبکه و اتصال بین‌المللی دیتاستر با بهره‌گیری از موقعیت استراتژیک خود در مجاورت فرودگاه و دسترسی به کابل‌های فیبر نوری بین‌المللی، خدمات شبکه پیشرفته‌ای ارائه می‌دهد: اتصال مستقیم به تبادل‌های اینترنتی (IXPs) منطقه‌ای و بین‌المللی برای کاهش تاخیر و هزینه ترافیک، سرویس‌های شبکه خصوصی مجازی (MPLS, SD-WAN) برای اتصال امن شعب مختلف شرکت‌ها، سرویس تحویل محتوا (CDN) با کش‌های لبه در نقاط استراتژیک برای تسریع دسترسی کاربران نهایی به محتوای پربازدید، و سرویس‌های تخصصی برای کاهش تاخیر (Low-Latency Solutions) برای کاربردهای حساس مانند معاملات مالی الکترونیکی و بازی‌های آنلاین. این خدمات به مشتریان امکان می‌دهد عملکرد جهانی خدمات دیجیتال خود را بهینه نمایند.

خدمت هفتم: مشاوره و ممیزی تخصصی دیتاستر و امنیت مرکز خدمات مشاوره‌ای تخصصی را در حوزه‌های ذیل ارائه می‌دهد: ارزیابی بلوغ زیرساخت فناوری اطلاعات مشتریان و ارائه نقشه راه بهینه‌سازی، مشاوره در زمینه انتخاب معماری ابری مناسب (عمومی، خصوصی، ترکیبی) و مهاجرت ایمن به ابر، انجام ممیزی‌های امنیتی و انطباق با استانداردهای بین‌المللی (ISO 27001, PCI-DSS, GDPR Principles) و ارائه گزارش شکاف و برنامه اصلاحی، و مشاوره در زمینه مدیریت انرژی دیتاستر و کاهش شاخص PUE. این خدمات توسط تیمی از مشاوران با تجربه عملیاتی در دیتاسترهای بزرگ و گواهینامه‌های بین‌المللی مرتبط ارائه می‌شود.

خدمت هشتم: خدمات ارزش افزوده برای اکوسیستم نوآوری دیتاستر به عنوان هسته اکوسیستم دیجیتال منطقه، خدمات ویژه‌ای برای استارت‌آپ‌ها و شرکت‌های نوآور ارائه می‌دهد: بسته‌های استارت‌آپی با تخفیف ویژه برای ۱۲ تا ۲۴ ماه اول فعالیت شامل فضای رک رایگان، اعتبار ابری، و پشتیبانی فنی اختصاصی؛ دسترسی به آزمایشگاه‌های تست و توسعه با تجهیزات تخصصی برای پروتوتایپینگ راه‌حل‌های جدید؛ تسهیل‌گری در جذب سرمایه از صندوق‌های خطرپذیر همکار از طریق رویدادهای دمو و شبکه‌سازی؛ و برنامه‌های منتورینگ توسط متخصصان باتجربه در حوزه‌های فنی و کسب و کاری. این خدمات به رشد سریع تر استارت‌آپ‌ها و ایجاد ارزش متقابل برای دیتاستر و اکوسیستم منجر می‌شود.

بخش نهم: جزئیات دقیق و عمیق فنی و عمرانی و انواع منابع مورد نیاز طرح

الف) جزئیات فنی و عمرانی زیرساخت فیزیکی دیتاستر:

۱. **مشخصات فنی ساختمان و سازه دیتاستر:** ساختمان دیتاستر با مساحت زیربنایی کل ۴۰۰۰ مترمربع در دو طبقه اصلی به همراه طبقات فنی و زیرزمین طراحی می‌شود. اسکلت ساختمان از نوع بتنی مسلح با سیستم قاب خمشی ویژه مطابق با آیین‌نامه ۲۸۰۰ ایران و استانداردهای بین‌المللی IBC 2021 برای مقاومت در برابر زلزله تا شدت ۸ ریشتر طراحی خواهد شد. کف سالن‌های میزبانی سرور (White Space) با بارگذاری حداقل ۱۲ کیلونیوتن بر مترمربع (معادل ۱۲۰۰ کیلوگرم بر مترمربع) برای تحمل وزن رک‌های پر ظرفیت و تجهیزات سنگین طراحی می‌شود. ارتفاع مفید سالن‌های سرور حداقل ۴.۵ متر از کف کاذب تا سقف کاذب در نظر گرفته می‌شود تا فضای کافی برای مسیرهای کابل کشی فوقانی، سیستم‌های خنک‌کنندگی و گردش هوا فراهم گردد.

کف کاذب سالن‌های سرور از نوع ضد لرزه با ارتفاع ۶۰ تا ۹۰ سانتی‌متر برای عبور کابل‌های برق و داده، و همچنین توزیع هوای خنک از زیر کف (Underfloor Air Distribution) استفاده می‌شود. سقف کاذب از پنل‌های معدنی غیر قابل اشتعال با عایق صوتی و حرارتی برای کنترل آکوستیک و جلوگیری از انتقال حرارت اجرا می‌گردد. دیوارهای داخلی سالن‌های سرور با پوشش ضد گردوغبار، ضد الکتریسیته ساکن (ESD-Protective) و با مقاومت در برابر رطوبت طراحی می‌شوند. درهای ورودی سالن‌های سرور از نوع ضد حریق با درجه مقاومت حداقل ۲ ساعت، مجهز به سیستم کنترل دسترسی بیومتریک و قفل‌های الکترومغناطیسی با پشتیبان باتری هستند.

۲. **سیستم‌های تأسیسات مکانیکی و خنک‌کنندگی:** سیستم خنک‌کنندگی دیتاستر با معماری ترکیبی و هوشمند طراحی می‌شود تا شاخص مصرف انرژی (PUE) به کمتر از ۱.۴ برسد. در فصول خنک سال (با دمای خارجی زیر ۱۸ درجه سانتی‌گراد)، از سیستم خنک‌کنندگی طبیعی (Free Cooling) با استفاده از هوای خارجی فیلتر شده و کنترل‌شده از نظر رطوبت استفاده می‌شود. در فصول گرم، از سیستم خنک‌کنندگی تبخیری غیرمستقیم (Indirect Evaporative Cooling) با راندمان بالا و مصرف آب بهینه بهره‌برداری می‌گردد. برای شرایط اوج بار حرارتی یا رطوبت بالا، چیلرهای جذبی یا تراکمی با مبرد دوستدار محیط‌زیست R-134a یا R-513A به‌عنوان پشتیبان فعال می‌شوند.

معماری توزیع هوا بر پایه اصل جداسازی مسیر هوای سرد و گرم (Hot/Cold Aisle Containment) طراحی می‌شود: رک‌های سرور به‌صورت ردیف‌های موازی با نمای جلو به راهرو سرد و نمای عقب به راهرو گرم چیده می‌شوند، و راهروها با درهای شیشه‌ای یا پنل‌های متحرک مسدود می‌گردند تا از اختلاط هوا جلوگیری شود. فن‌های هوشمند با قابلیت کنترل دور متغیر (EC Fans) بر اساس بار حرارتی واقعی هر منطقه، مصرف برق سیستم خنک‌کنندگی را بهینه می‌نمایند. سنسورهای دما و رطوبت در نقاط استراتژیک سالن سرور (ورودی و خروجی هر رک، مسیرهای هوای سرد و گرم) نصب شده و داده‌ها به سیستم مدیریت زیرساخت دیتاستر (DCIM) ارسال می‌گردند.

۳. **سیستم‌های تأسیسات الکتریکی و توزیع برق:** سیستم برق‌رسانی دیتاستر با افزونگی کامل ۲N یا ۱N+۱ بسته به بخش طراحی می‌شود تا تداوم برق بدون وقفه تضمین گردد. برق ورودی از دو منبع مستقل شبکه سراسری با پست‌های توزیع مجزا تأمین می‌شود. تابلوهای توزیع اصلی (MV/LV Switchgear) با کلیدهای اتوماتیک هوشمند و قابلیت سوئیچینگ

خودکار بین منابع، بار را بین ترانسفورماتورها متعادل می نمایند. ترانسفورماتورهای خشک با ظرفیت 2×2500 کیلوولت آمپر با راندمان بالا و سطح عایقی مناسب برای محیط دیتاستر انتخاب می شوند.

سیستم برق اضطراری شامل ژنراتورهای دیزلی صنعتی با ظرفیت 2×2000 کیلووات به پیکربندی $N+1$ ، مجهز به سیستم های شروع خودکار در کمتر از ۱۰ ثانیه پس از قطع برق اصلی، و با مخازن سوخت کافی برای حداقل ۷۲ ساعت کارکرد پیوسته است. بانک باتری های UPS از نوع VRLA یا لیتیوم-یون با ظرفیت ۱۰۰۰ کیلووات-ساعت، زمان پشتیبانی ۱۵ تا ۳۰ دقیقه ای برای پوشش فاصله تا راه اندازی ژنراتورها و همچنین فیلتر کردن نوسانات برق را فراهم می آورد. سیستم توزیع برق در سالن سرور از نوع Busway یا PDU های هوشمند رک مونت با قابلیت مانیتورینگ مصرف هر رک و هر فاز، و امکان خاموش/روشن کردن از راه دور پریزها است.

۴. سیستم های امنیتی فیزیکی و کنترل دسترسی: سیستم امنیتی فیزیکی دیتاستر با رویکرد لایه ای (Defense in Depth) طراحی می شود: لایه اول شامل حصارکشی محیطی با سنسورهای لرزه ای و دوربین های حرارتی برای تشخیص نفوذ از فاصله دور؛ لایه دوم شامل کنترل ورودی اصلی ساختمان با گیت های امنیتی، اسکنرهای بدنی و بازرسی کیف؛ لایه سوم شامل کنترل دسترسی به سالن های سرور با سیستم بیومتریک چندعاملی (اثر انگشت + تشخیص چهره + کارت هوشمند) و ثبت دقیق زمان ورود و خروج هر فرد؛ لایه چهارم شامل قفل های الکترونیکی روی هر رک سرور با امکان بازگشایی فقط توسط پرسنل مجاز و ثبت لاگ دسترسی.

دوربین های مدار بسته با رزولوشن K4، قابلیت دید در شب، و تحلیل هوشمند تصویر (تشخیص حرکت غیرعادی، رها شدن شیء، تجمع افراد) در تمامی نقاط حساس نصب می شوند و تصاویر به صورت بلادرنگ به مرکز کنترل امنیت SOC فیزیکی ارسال می گردند. سیستم اعلام و اطفاء حریق از نوع آدرس پذیر با دکتورهای دود، حرارت و شعله در تمامی فضاها، و سیستم اطفاء گازی Novec 1230 یا FM200 در سالن های سرور و اتاق های برق با زمان تخلیه کمتر از ۱۰ ثانیه و بدون باقیمانده مخرب برای تجهیزات الکترونیکی طراحی می شود.

ب) منابع انسانی مورد نیاز با جزئیات تخصصی:

۱. تیم مدیریت ارشد و راهبردی:

- مدیرعامل دیتاستر: دارای حداقل ۱۵ سال تجربه مدیریتی در حوزه مراکز داده، خدمات ابری یا زیرساخت های فناوری اطلاعات، ترجیحاً با سابقه کار در دیتاسترهای گرید بالا بین المللی، دارای مدرک کارشناسی ارشد یا دکترا در رشته های مهندسی کامپیوتر، مهندسی صنایع، مدیریت فناوری اطلاعات یا رشته های مرتبط.
- مدیر فنی و عملیات (CTO/COO): دارای حداقل ۱۲ سال تجربه در طراحی، راه اندازی و بهره برداری از دیتاسترهای بزرگ، با تسلط بر استانداردهای TIA-942, ISO 27001 مدیریت ظرفیت و بهینه سازی انرژی، و تجربه رهبری تیم های فنی چند تخصصی.

- مدیر امنیت سایبری (CISO): دارای تخصص در امنیت زیرساخت‌های حیاتی، گواهینامه‌های بین‌المللی CISSP, CISM, تجربه در طراحی معماری امنیتی لایه‌ای، مدیریت حوادث سایبری و انطباق با مقررات حاکمیتی.
- مدیر تجاری و توسعه کسب و کار: دارای تجربه در بازاریابی خدمات زیرساختی و ابری، مذاکره قراردادهای بزرگ با مشتریان استراتژیک، و توسعه مشارکت‌های بین‌المللی در حوزه فناوری اطلاعات.
- مدیر مالی و سرمایه‌گذاری: دارای تخصص در مدیریت مالی پروژه‌های زیرساختی بزرگ، مدل‌سازی مالی خدمات ابری، و جذب سرمایه‌گذاری با ساختارهای ترکیبی داخلی و بین‌المللی.

۲. تیم‌های تخصصی فنی و عملیاتی:

- تیم عملیات دیتاسنتر: شامل ۱۵ تا ۲۰ تکنسین و مهندس با تخصص در مدیریت سرورهای لینوکس/ویندوز، پیکربندی شبکه، عیب‌یابی سخت‌افزار، و پاسخ به حوادث فیزیکی، با توانایی کار در شیفت‌های ۷/۲۴.
- تیم شبکه و ارتباطات: شامل ۸ تا ۱۲ مهندس شبکه با گواهینامه‌های تخصصی (CCNP, CCIE, JNCIP) و تجربه در پیکربندی سوئیچ‌های هسته، مسیریابی BGP، و مدیریت ترافیک بین‌المللی.
- تیم امنیت سایبری و SOC: شامل ۱۰ تا ۱۵ متخصص امنیت با گواهینامه‌های بین‌المللی (CEH, OSCP, GCFA)، تجربه در تحلیل تهدیدات، پاسخ به حوادث، و پایش بلادرنگ با ابزارهای SIEM/SOAR.
- تیم خدمات ابری و توسعه پلتفرم: شامل ۱۲ تا ۱۸ مهندس نرم‌افزار و دواپس با تخصص در فناوری‌های مجازی‌سازی (VMware, KVM)، کانتینرها (Docker, Kubernetes)، و اتوماسیون زیرساخت (Terraform, Ansible).
- تیم پشتیبانی مشتریان و خدمات فنی: شامل ۱۰ تا ۱۵ کارشناس با مهارت‌های فنی و ارتباطی قوی برای پاسخگویی به درخواست‌ها، عیب‌یابی اولیه، و هماهنگی با تیم‌های تخصصی برای حل مسائل پیچیده.
- تیم مدیریت انرژی و پایداری: شامل ۳ تا ۵ مهندس مکانیک و برق با تخصص در بهینه‌سازی مصرف انرژی دیتاسنتر، تحلیل داده‌های سنسورها، و پیاده‌سازی راه‌حل‌های سبز.

۳. تیم پشتیبانی و خدمات:

- تیم تأسیسات و نگهداری: شامل ۸ تا ۱۲ تکنسین برق، مکانیک و تأسیسات با تجربه در نگهداری پیشگیرانه (Preventive Maintenance) سیستم‌های حیاتی دیتاسنتر.
- تیم امنیت فیزیکی: شامل ۱۰ تا ۱۵ نگهبان آموزش‌دیده تخصصی دیتاسنتر با گواهینامه‌های امنیتی و توانایی کار در شیفت‌های چرخشی.
- تیم اداری، مالی و منابع انسانی: شامل ۶ تا ۸ کارشناس با تجربه در محیط‌های فناوری محور و آشنایی با استانداردهای گزارش‌دهی بین‌المللی.

ج) منابع دانشی، مهارتی و فناورانه:

۱. دانش و مالکیت فکری مورد نیاز:

- دسترسی به پایگاه‌های دانش تخصصی شامل استانداردهای فنی دیتاسنتر, (TIA-942, EN 50600) استانداردهای امنیت اطلاعات, (ISO 27001, NIST CSF) و بهترین روش‌های صنعت از طریق اشتراک در پلتفرم‌هایی مانند Uptime Institute, 451 Research, Gartner Data Center Insights.
- توسعه و ثبت مالکیت فکری استراتژیک شامل الگوریتم‌های بومی بهینه‌سازی مصرف انرژی دیتاسنتر بر اساس اقلیم ایران, پروتکل‌های امنیتی تطبیقی برای تهدیدات منطقه‌ای, و چارچوب‌های مدیریت هوشمند ظرفیت مبتنی بر هوش مصنوعی.
- ایجاد کتابخانه کد باز (Open Source Repository) داخلی برای ابزارهای مدیریت زیرساخت, مانیتورینگ و اتوماسیون, با رعایت سیاست‌های امنیتی و امکان همکاری با جامعه جهانی توسعه‌دهندگان.

۲. مهارت‌های تخصصی و برنامه توسعه توانمندی:

- طراحی مسیر توسعه شغلی (Career Path) و برنامه آموزش مستمر (Continuous Learning) برای کلیه کارکنان شامل دوره‌های داخلی, شرکت در کنفرانس‌های بین‌المللی دیتاسنتر مانند Data Center Dynamics, Cloud Expo, و فرصت‌های مبادله تخصصی با دیتاسنترهای همکار جهانی.
- استقرار سیستم ارزیابی عملکرد مبتنی بر شایستگی (Competency-Based Assessment) برای شناسایی شکاف‌های مهارتی و برنامه‌ریزی هدفمند توسعه فردی و تیمی, با تمرکز بر مهارت‌های حیاتی مانند مدیریت حوادث, بهینه‌سازی انرژی, و امنیت سایبری.
- ایجاد برنامه جانشین‌پروری (Succession Planning) برای پست‌های کلیدی فنی و مدیریتی جهت تضمین تداوم دانش سازمانی و کاهش ریسک وابستگی به افراد, همراه با مستندسازی فرآیندهای حیاتی و ایجاد بانک دانش فنی.

(د) منابع فیزیکی، تجهیزات و تکنولوژی:

۱. تجهیزات سخت‌افزاری و زیرساخت فیزیکی:

- رک‌های سرور: ۸۰۰ رک استاندارد ۴۲ یونیتی با عمق ۱۲۰۰ میلی‌متر, ظرفیت بارگذاری ۱۵۰۰ کیلوگرم, مجهز به سیستم‌های مدیریت کابل عمودی و افقی, و قفل‌های الکترونیکی با کنترل دسترسی.
- سرورهای محاسباتی: ۴۰۰ تا ۶۰۰ سرور رک‌مونت با پردازنده‌های Intel Xeon Scalable یا AMD EPYC نسل جدید, حافظه RAM حداقل ۲۵۶ گیگابایت, و ذخیره‌سازی NVMe با ظرفیت حداقل ۱۰ ترابایت برای هر سرور در پیکربندی‌های مختلف برای خدمات IaaS.
- سیستم‌های ذخیره‌سازی: آرایه‌های ذخیره‌سازی SAN/NAS با ظرفیت اولیه ۵ پتابایت, پشتیبانی از پروتکل‌های FC, iSCSI, NFS, SMB, و قابلیت تکرار داده بلادرنگ (Synchronous/Asynchronous Replication) به سایت پشتیبان.

- تجهیزات شبکه: سوئیچ‌های هسته با پورت‌های ۱۰۰ GbE و پشتیبانی از VXLAN/EVPN برای شبکه‌های ابری، سوئیچ‌های دسترسی با پورت‌های ۱۰/۱۰/۱ GbE، روترهای لبه با پشتیبانی از BGP و MPLS، و فایروال‌های نسل جدید با توان پردازش تراکنش بالا.
- سیستم‌های خنک‌کنندگی: واحدهای خنک‌کننده دقیق (CRAH/CRAC) با ظرفیت کل ۳ مگاوات حرارتی، فن‌های EC با کنترل دور متغیر، سیستم‌های کنترل رطوبت، و سنسورهای محیطی هوشمند در هر ردیف رک.
- سیستم‌های برق: تابلوهای توزیع هوشمند، UPS‌های ماژولار با قابلیت توسعه، ژنراتورهای دیزلی با سیستم‌های کنترل پیشرفته، و بانک‌های باتری لیتیوم-یون با عمر مفید طولانی‌تر.

۲. نرم‌افزارها و پلتفرم‌های تخصصی:

- سیستم مدیریت زیرساخت دیتاسنتر (DCIM): پلتفرم‌هایی مانند Nlyte, Sunbird یا Device42 برای مانیتورینگ بلادرنگ ظرفیت، انرژی، دما، و تولید گزارش‌های تحلیلی بهینه‌سازی.
- پلتفرم مجازی‌سازی و ابر: VMware vCloud Suite یا OpenStack برای ارائه خدمات IaaS، همراه با Kubernetes برای اورکستراسیون کانتینرها و سرویس‌های PaaS.
- سیستم‌های امنیت سایبری: پلتفرم SIEM مانند Splunk یا IBM QRadar برای همبستگی لاگ‌ها، سیستم‌های EDR برای تشخیص و پاسخ به تهدیدات در نقطه پایانی، و ابزارهای اسکن آسیب‌پذیری مانند Tenable یا Qualys.
- ابزارهای اتوماسیون و دواپس: Ansible, Terraform, Jenkins برای اتوماسیون تأمین و پیکربندی زیرساخت، و Prometheus/Grafana برای مانیتورینگ عملکرد برنامه‌ها.
- نرم‌افزارهای مدیریت خدمت: پلتفرم ITSM مبتنی بر ITIL 4 مانند ServiceNow یا Jira Service Management برای مدیریت درخواست‌ها، حوادث، تغییرات و دارایی‌های فناوری اطلاعات.

ه) مواد اولیه و منابع مصرفی:

- قطعات بدکی استراتژیک: ماژول‌های حافظه، دیسک‌های SSD/HDD، کارت‌های شبکه، منبع تغذیه، و فن‌های رک با موجودی کافی برای حداقل ۶ ماه عملیات بدون وقفه، همراه با سیستم مدیریت موجودی هوشمند برای پیش‌بینی نیازها.
- مواد مصرفی تأسیسات: فیلترهای هوای HEPA برای سیستم‌های خنک‌کنندگی، مایعات خنک‌کننده و ضدیخ، مواد شیمیایی تصفیه آب برج‌های خنک‌کننده، و گازهای اطفاء حریق با برنامه جایگزینی دوره‌ای بر اساس توصیه‌های سازنده.
- مواد و تجهیزات امنیتی: کارت‌های دسترسی هوشمند، حسگرهای بیومتریک یدکی، لنز و تجهیزات دوربین‌های مداربسته، و باتری‌های پشتیبان سیستم‌های کنترل دسترسی با برنامه به‌روزرسانی فناوری هر ۳ تا ۵ سال.
- مواد مصرفی اداری و عملیاتی: تجهیزات حفاظت فردی برای پرسنل فنی، مواد ضدالکتریسیته ساکن برای کار با تجهیزات حساس، و ملزومات بسته‌بندی و حمل تجهیزات.

و) عوامل محیطی و ملاحظات پایداری:

- سیستم پایش بلادرننگ کیفیت هوا، دما و رطوبت در محیط دیتاستر و پیرامون آن با حسگرهای IoT و گزارش‌دهی خودکار به سامانه‌های نظارتی زیست‌محیطی و داخلی.
- برنامه مدیریت پسماند الکترونیکی با همکاری شرکت‌های مجاز بازیافت برای جمع‌آوری، تفکیک و پردازش ایمن تجهیزات فرسوده مطابق با استانداردهای WEEE، با هدف دستیابی به نرخ بازیافت بالای ۹۰٪ و مستندسازی کامل فرآیند.
- سیستم جمع‌آوری و استفاده از آب باران برای مصارف غیرشرب و آبیاری فضای سبز، همراه با تصفیه‌خانه کوچک‌مقیاس برای بازیافت آب خاکستری و چرخش آب در سیستم‌های خنک‌کنندگی تبخیری.
- برنامه کاشت درختان بومی و ایجاد فضای سبز عمودی در ساختمان برای کاهش اثر جزیره گرمایی شهری، بهبود کیفیت هوا و ایجاد محیط کاری الهام‌بخش، همراه با پایش شاخص‌های سبز و گزارش‌دهی سالانه.

بخش دهم: استانداردهای الزامی و اختیاری

الف) استانداردهای الزامی (Mandatory Standards):

۱. استانداردهای فنی دیتاستر و زیرساخت:

- استاندارد طراحی و ارزیابی دیتاستر ANSI/TIA-942-B برای گرید Tier III با الزامات مربوط به افزودنی تجهیزات برق و خنک‌کنندگی، مسیرهای توزیع مستقل، و دسترسی‌پذیری حداقل ۹۹.۹۸۲٪، همراه با مستندات طراحی برای امکان ارتقا به Tier IV در آینده.
- استاندارد سیستم‌های زمین کردن و پیوندینگ در دیتاستر ANSI/TIA-607-B برای حفاظت تجهیزات در برابر صاعقه، نوسانات برق و تخلیه الکترواستاتیک، با مقاومت زمین کمتر از ۱ اهم.
- استاندارد کابل‌کشی ساختاریافته برای مراکز داده ANSI/TIA-568.0-D با پشتیبانی از فیبر نوری چندحالتی و تک‌حالتی برای پهنای باندهای بالا و فواصل طولانی.
- استاندارد مدیریت ظرفیت و انرژی دیتاستر ISO/IEC 30134 سری استانداردهای PUE, ERE, CUE برای پایش و گزارش‌دهی شاخص‌های بهره‌وری انرژی و محیط‌زیستی.

۲. استانداردهای امنیت اطلاعات و سایبری:

- استاندارد سیستم مدیریت امنیت اطلاعات ISO/IEC 27001:2022 برای استقرار چارچوب جامع حفاظت از داده‌های حساس مشتریان، شامل کنترل‌های دسترسی، رمزنگاری، مدیریت حوادث و انطباق قانونی.
- استاندارد امنیت پرداخت کارت‌های پرداخت PCI-DSS v4.0 برای هرگونه میزبانی یا پردازش داده‌های کارت‌های پرداخت، شامل الزامات شبکه امن، رمزنگاری داده‌ها، پایش دسترسی و تست امنیتی دوره‌ای.
- چارچوب امنیت سایبری مؤسسه ملی استانداردها و فناوری آمریکا (NIST Cybersecurity Framework) برای شناسایی، حفاظت، تشخیص، پاسخ و بازیابی در برابر تهدیدات سایبری با رویکرد ریسک‌محور.

- استاندارد رمزنگاری ماژول‌های امنیتی FIPS 140-3 برای تجهیزات و نرم‌افزارهای رمزنگاری مورد استفاده در سیستم‌های حساس، به‌ویژه در مدیریت کلیدها و احراز هویت.

۳. استانداردهای مدیریت خدمت و عملیات:

- استاندارد مدیریت خدمات فناوری اطلاعات ISO/IEC 20000-1:2018 برای استقرار فرآیندهای مدیریت خدمت مبتنی بر بهترین روش‌های ITIL 4 و تضمین کیفیت خدمات ارائه‌شده به مشتریان با قراردادهای سطح سرویس شفاف.
- استاندارد مدیریت تداوم کسب‌وکار ISO 22301:2019 برای طراحی و آزمون برنامه‌های بازیابی فاجعه و تضمین تداوم خدمات حیاتی در شرایط اختلال با زمان بازیابی تعریف‌شده.
- استاندارد ایمنی و بهداشت حرفه‌ای ISO 45001:2018 برای حفاظت از سلامت و ایمنی کارکنان در محیط فیزیکی دیتاسنتر شامل کار با تجهیزات برق فشارقوی، سیستم‌های خنک‌کنندگی و عملیات نگهداری.

۴. استانداردهای حاکمیتی و انطباق مقرراتی ایران:

- الزامات امنیتی مرکز افتای ریاست جمهوری برای مراکز داده درجه ۱ و ۲ شامل کنترل‌های فیزیکی، منطقی و فرآیندی برای میزبانی داده‌های حساس حاکمیتی و تجاری.
- مقررات سازمان تنظیم مقررات و ارتباطات رادیویی برای ارائه خدمات ارتباطی و داده‌ای شامل مجوزهای فنی، گزارش‌دهی ترافیک و رعایت سیاست‌های حاکمیت داده.
- قانون تجارت الکترونیک و قانون حمایت از داده‌های شخصی (در صورت تصویب نهایی) شامل اصول پردازش قانونی داده، حقوق ذی‌نفعان و گزارش‌دهی نقض داده.

ب) استانداردهای اختیاری و توصیه‌شده (Optional/Recommended Standards):

۱. استانداردهای پایداری و تعالی عملیاتی:

- استاندارد مدیریت محیط زیست ISO 14001:2015 برای پایش و کاهش اثرات زیست‌محیطی فعالیت‌های دیتاسنتر و حرکت به سمت عملیات کربن‌خنثی با برنامه‌های کاهش انتشار.
- استانداردهای ساختمان سبز LEED v4.1 Data Centers یا BREEAM Data Centres برای طراحی و بهره‌برداری پایدار از ساختمان دیتاسنتر با تمرکز بر بهره‌وری انرژی، مدیریت آب و کیفیت محیط داخلی.
- چارچوب گزارش‌دهی پایداری GRI Standards و استاندارد افشای مالی مرتبط با آب‌وهوا TCFD برای شفاف‌سازی عملکرد اقتصادی، اجتماعی و زیست‌محیطی دیتاسنتر در گزارش‌های سالانه.

۲. استانداردهای تخصصی ابر و فناوری‌های نوظهور:

- استانداردهای قابلیت تعامل ابری CSA STAR و ISO/IEC 19941 برای اطمینان از پرتابلیتی داده و برنامه بین پلتفرم‌های ابری مختلف و کاهش وابستگی به تأمین‌کننده خاص.

- چارچوب‌های حاکمیت داده و اخلاق هوش مصنوعی مانند EU Ethics و OECD AI Principles
- Guidelines for Trustworthy AI برای توسعه مسئولانه و شفاف سیستم‌های هوش مصنوعی در خدمات مدیریت دیتاستر.

- استانداردهای باز برای API های مدیریت ابر مانند OpenStack API, Kubernetes API و Cloud Events
- برای تسهیل یکپارچه‌سازی با ابزارهای مشتریان و اکوسیستم توسعه‌دهندگان.

۳. استانداردهای مدیریت پروژه و نوآوری:

- راهنمای بدنه دانش مدیریت پروژه PMBOK Guide هفتمین ویرایش یا استاندارد ISO 21502 برای مدیریت حرفه‌ای پروژه‌های توسعه و بهره‌برداری دیتاستر با تمرکز بر تحویل ارزش.
- چارچوب چابک (Agile) و اسکرام (Scrum) با تطبیق برای محیط‌های عملیاتی زیرساختی (DevOps/SRE) برای تسریع توسعه خدمات جدید با حفظ پایداری و امنیت.
- استاندارد مدیریت نوآوری ISO 56002:2019 برای استقرار سیستم مدیریت نوآوری سیستماتیک در حوزه بهینه‌سازی انرژی، امنیت سایبری و خدمات ارزش افزوده دیتاستر.

ج) مکانیزم انطباق و ممیزی استانداردها:

- ایجاد واحد مستقل انطباق و ممیزی داخلی با مسئولیت پایش مستمر رعایت استانداردهای الزامی، انجام ممیزی‌های دوره‌ای داخلی، و هماهنگی با ممیزان خارجی معتبر مانند Bureau Veritas, DNV, BSI برای اخذ و تمدید گواهینامه‌های بین‌المللی.
- استقرار پلتفرم مدیریت انطباق (Compliance Management Platform) برای مستندسازی سیاست‌ها، فرآیندها و شواهد انطباق، مدیریت ریسک‌های عدم انطباق، و تولید خودکار گزارش‌های نظارتی برای نهادهای حاکمیتی.
- طراحی برنامه آموزش اجباری سالانه برای کلیه کارکنان در زمینه استانداردهای مرتبط با نقش‌های شغلی آنان و ارزیابی اثربخشی آموزش از طریق آزمون‌های عملی، شبیه‌سازی سناریوهای انطباق و ممیزی‌های داخلی.
- ایجاد مکانیزم گزارش‌دهی شفاف به ذی‌نفعان شامل انتشار سالانه گزارش انطباق و پایداری، و برگزاری جلسات پرسش و پاسخ با مشتریان استراتژیک و نهادهای نظارتی برای افزایش اعتماد و شفافیت.

بخش یازدهم: ساختار تفصیلی حجم سرمایه، ساختار تفصیلی هزینه‌های عملیاتی، شاخص‌های کلیدی تحلیل مالی و اقتصادی

الف) ساختار تفصیلی حجم سرمایه‌گذاری اولیه (۴۵ میلیون یورو):

۱. سرمایه‌گذاری ثابت و زیرساختی (۲۸ میلیون یورو - ۶۲.۲٪ کل سرمایه):

- احداث و تجهیز ساختمان دیتاسنتر (۴۰۰۰ مترمربع): ۱۲ میلیون یورو شامل هزینه‌های طراحی معماری تخصصی دیتاسنتر و مهندسی تأسیسات (۱.۵ میلیون یورو)، عملیات خاکی، فونداسیون و اسکلت بتنی مسلح با بارگذاری ویژه (۴ میلیون یورو)، نازک کاری تخصصی شامل کف کاذب ضد لرزه، دیوارهای ضد گردوغبار و عایق‌بندی حرارتی-صوتی (۳ میلیون یورو)، تأسیسات مکانیکی و الکتریکی پایه (۲.۵ میلیون یورو)، و سیستم‌های امنیتی فیزیکی و هوشمندسازی ساختمان (۱ میلیون یورو).
- راه‌اندازی سیستم‌های خنک‌کنندگی و مدیریت انرژی: ۶ میلیون یورو شامل واحدهای خنک‌کننده دقیق (CRAH/CRAC) با معماری Hot/Cold Aisle Containment (۳ میلیون یورو)، سیستم‌های خنک‌کنندگی طبیعی و تبخیری غیرمستقیم (۱.۵ میلیون یورو)، سنسورهای محیطی هوشمند و سیستم مدیریت انرژی یکپارچه (۱ میلیون یورو)، و سیستم‌های بازیافت آب و بهینه‌سازی مصرف (۰.۵ میلیون یورو).
- تأمین سیستم‌های برق و توزیع انرژی: ۵ میلیون یورو شامل ترانسفورماتورهای خشک با ظرفیت ۲۵۰۰×۲ کیلوولت‌آمپر (۱.۵ میلیون یورو)، تابلوهای توزیع هوشمند و سیستم‌های سوئیچینگ خودکار (۱ میلیون یورو)، ژنراتورهای دیزلی N+1 با ظرفیت ۲۰۰۰×۲ کیلووات و مخازن سوخت (۱.۵ میلیون یورو)، و بانک‌های باتری UPS با ظرفیت ۱۰۰۰ کیلووات-ساعت (۱ میلیون یورو).
- تجهیزات شبکه و امنیت سایبری پایه: ۳ میلیون یورو شامل سوئیچ‌های هسته و توزیع با ظرفیت ۱۰۰ گیگابیت بر ثانیه (۱.۵ میلیون یورو)، فایروال‌های نسل جدید و سیستم‌های تشخیص نفوذ (۱ میلیون یورو)، و سیستم‌های مدیریت هویت و دسترسی (۰.۵ میلیون یورو).
- هزینه‌های پیش‌بینی نشده و ذخیره احتیاطی زیرساخت: ۲ میلیون یورو برای پوشش ریسک‌های اجرایی، نوسانات قیمت تجهیزات وارداتی، و نیازهای غیرمترقبه در فاز راه‌اندازی.

۲. سرمایه‌گذاری در تجهیزات فعال و پلتفرم‌های نرم‌افزاری (۱۰ میلیون یورو - ۲۲.۲٪ کل سرمایه):

- سرورها و سیستم‌های ذخیره‌سازی اولیه: ۶ میلیون یورو شامل ۴۰۰ سرور رک‌مونت با پیکربندی‌های متنوع برای خدمات IaaS (۴ میلیون یورو)، آرایه‌های ذخیره‌سازی SAN/NAS با ظرفیت اولیه ۵ پتابایت (۱.۵ میلیون یورو)، و تجهیزات بک‌آپ و تکرار داده (۰.۵ میلیون یورو).
- پلتفرم‌های مجازی‌سازی و خدمات ابری: ۲ میلیون یورو شامل لایسنس‌های VMware vCloud Suite یا پلتفرم OpenSource با پشتیبانی تجاری (۱ میلیون یورو)، پلتفرم مدیریت کانتینر Kubernetes با ابزارهای مرتبط (۰.۵ میلیون یورو)، و سیستم‌های اتوماسیون و اورکستراسیون (۰.۵ میلیون یورو).
- نرم‌افزارهای مدیریت و امنیت: ۲ میلیون یورو شامل پلتفرم DCIM برای مدیریت زیرساخت (۰.۸ میلیون یورو)، سیستم SIEM برای مدیریت رویدادهای امنیتی (۰.۷ میلیون یورو)، پلتفرم ITSM مبتنی بر ITIL (۰.۳ میلیون یورو)، و ابزارهای مانیتورینگ و تحلیل عملکرد (۰.۲ میلیون یورو).

۳. سرمایه در گردش و هزینه‌های راه‌اندازی عملیاتی (۴ میلیون یورو - ۸.۹٪ کل سرمایه):

- هزینه‌های جذب و آموزش نیروی انسانی تخصصی: ۱.۵ میلیون یورو شامل هزینه‌های استخدام تیم مدیریت ارشد و متخصصان با تجربه بین‌المللی (۰.۸ میلیون یورو)، برنامه‌های آموزش تخصصی و گواهینامه‌های بین‌المللی برای کارکنان فنی (۰.۵ میلیون یورو)، و هزینه‌های جابجایی و اسکان اولیه نیروهای کلیدی (۰.۲ میلیون یورو).
- هزینه‌های اخذ مجوزها، گواهینامه‌ها و مشاوره تخصصی: ۱.۲ میلیون یورو شامل هزینه‌های مشاوره با متخصصان بین‌المللی دیتاستر و امنیت سایبری (۰.۶ میلیون یورو)، اخذ گواهینامه‌های ISO توسط ممیزان معتبر (۰.۴ میلیون یورو)، و هزینه‌های اخذ مجوزهای حاکمیتی از سازمان تنظیم مقررات و مرکز افا (۰.۲ میلیون یورو).
- هزینه‌های بازاریابی، برندینگ و جذب مشتریان استراتژیک: ۰.۸ میلیون یورو شامل طراحی و اجرای کمپین‌های تخصصی جذب مشتریان بزرگ (۰.۴ میلیون یورو)، شرکت در کنفرانس‌ها و رویدادهای بین‌المللی دیتاستر و ابر (۰.۳ میلیون یورو)، و توسعه پلتفرم‌های دیجیتال مارکتینگ و تولید محتوای تخصصی (۰.۱ میلیون یورو).
- سرمایه در گردش اولیه برای پوشش هزینه‌های عملیاتی ۱۲ ماه اول: ۰.۵ میلیون یورو برای تأمین نقدینگی مورد نیاز تا زمان تحقق درآمدهای پایدار از مشتریان اولیه.

۴. هزینه‌های تحقیق و توسعه و نوآوری (۳ میلیون یورو - ۶.۷٪ کل سرمایه):

- بودجه تحقیق و توسعه در حوزه بهینه‌سازی انرژی: ۱.۵ میلیون یورو برای توسعه الگوریتم‌های هوش مصنوعی مدیریت مصرف انرژی بر اساس اقلیم ایران، تست سیستم‌های خنک‌کنندگی نوین، و ثبت اختراعات مرتبط.
- بودجه تحقیق و توسعه در حوزه امنیت سایبری: ۱ میلیون یورو برای توسعه راه‌حل‌های بومی تشخیص تهدیدات منطقه‌ای، پروتکل‌های رمزنگاری تطبیقی، و ابزارهای تست نفوذ خودکار.
- بودجه همکاری‌های پژوهشی و انتقال فناوری: ۰.۵ میلیون یورو برای انعقاد تفاهم‌نامه با دانشگاه‌ها و مراکز تحقیقاتی، شرکت در پروژه‌های پژوهشی بین‌المللی، و جذب استارت‌آپ‌های نوآور در حوزه دیتاستر.

ب) ساختار تفصیلی هزینه‌های عملیاتی سالانه (پس از بهره‌برداری کامل):

۱. هزینه‌های پرسنلی و نیروی انسانی (سالانه ۳.۲ میلیون یورو):

- حقوق و مزایای تیم مدیریت ارشد (۵ نفر): ۰.۹ میلیون یورو با میانگین حقوق سالانه ۱۸۰,۰۰۰ یورو برای هر نفر شامل حقوق پایه، پاداش عملکرد و مزایای غیرنقدی.
- حقوق و مزایای تیم‌های تخصصی فنی، امنیتی و عملیاتی (۸۰ نفر): ۱.۸ میلیون یورو با میانگین حقوق سالانه ۲۲,۵۰۰ یورو برای هر نفر با در نظر گیری سطوح مختلف تجربه و تخصص.
- هزینه‌های آموزش مستمر، گواهینامه‌های بین‌المللی و توسعه حرفه‌ای کارکنان: ۰.۳ میلیون یورو.
- هزینه‌های رفاهی، بیمه تکمیلی، پاداش‌های عملکردی و برنامه‌های حفظ نیروی انسانی نخبه: ۰.۲ میلیون یورو.

۲. هزینه‌های انرژی و تأسیسات (سالانه ۲.۱ میلیون یورو):

- هزینه برق مصرفی دیتاستر: ۱.۵ میلیون یورو با پیش‌بینی مصرف سالانه ۱۰ گیگاوات‌ساعت و نرخ متوسط برق صنعتی در منطقه آزاد، با در نظر گیری کاهش تدریجی مصرف از طریق بهینه‌سازی و استفاده از انرژی خورشیدی.
- هزینه سوخت ژنراتورها و نگهداری سیستم‌های برق اضطراری: ۰.۳ میلیون یورو شامل سوخت دیزل برای تست‌های دوره‌ای و شرایط اضطراری، و قراردادهای نگهداری پیشگیرانه.
- هزینه آب مصرفی سیستم‌های خنک‌کنندگی و تصفیه: ۰.۲ میلیون یورو با در نظر گیری سیستم‌های بازیافت و چرخش آب برای کاهش مصرف.
- هزینه نگهداری و تعمیرات پیشگیرانه تأسیسات مکانیکی و الکتریکی: ۰.۱ میلیون یورو.

۳. هزینه‌های فناوری اطلاعات و امنیت سایبری (سالانه ۱.۴ میلیون یورو):

- هزینه‌های لایسنس سالانه نرم‌افزارهای تخصصی (مجازی‌سازی، مدیریت، امنیت): ۰.۶ میلیون یورو.
- هزینه‌های به‌روزرسانی سخت‌افزار، جایگزینی قطعات مصرفی و ارتقای تدریجی تجهیزات: ۰.۴ میلیون یورو.
- هزینه‌های خدمات امنیتی خارجی شامل تست نفوذ دوره‌ای، ممیزی امنیتی مستقل، و اشتراک سرویس‌های تهدیدسنجی بلادرنگ: ۰.۳ میلیون یورو.
- هزینه‌های پهنای باند بین‌المللی و اتصال به تبادل‌های اینترنتی: ۰.۱ میلیون یورو.

۴. هزینه‌های اداری، بازاریابی و عمومی (سالانه ۰.۷ میلیون یورو):

- هزینه‌های خدمات نظافتی تخصصی دیتاستر، امنیت فیزیکی برون‌سپاری‌شده، و پشتیبانی اداری: ۰.۳ میلیون یورو.
- هزینه‌های بازاریابی تخصصی، تولید محتوا، و حضور در رویدادهای صنعتی: ۰.۲ میلیون یورو.
- هزینه‌های بیمه‌های تخصصی شامل بیمه تجهیزات، بیمه مسئولیت حرفه‌ای، و بیمه ریسک سایبری: ۰.۱۵ میلیون یورو.
- هزینه‌های سفرهای کاری تخصصی، ارتباطات و هماهنگی با شرکای بین‌المللی: ۰.۰۵ میلیون یورو.

جمع کل هزینه‌های عملیاتی سالانه در وضعیت بهره‌برداری کامل: ۷.۴ میلیون یورو

ج) شاخص‌های کلیدی تحلیل مالی و اقتصادی:

۱. پیش‌بینی درآمدها و جریان‌های نقدی ورودی:

- درآمدهای حاصل از خدمات میزبانی رک (Colocation): پیش‌بینی اشغال ۷۰٪ ظرفیت ۸۰۰ رک در سال سوم بهره‌برداری با میانگین درآمد ماهانه ۸۰۰ یورو برای هر رک (شامل فضای فیزیکی، برق ۵ کیلووات، خنک‌کنندگی و پهنای باند پایه)، منجر به درآمد سالانه حدود ۵.۳۸ میلیون یورو.
- درآمدهای حاصل از خدمات ابری IaaS/PaaS: پیش‌بینی جذب ۲۰۰ مشتری فعال با میانگین مصرف ماهانه ۱,۵۰۰ یورو بر اساس مدل پرداخت بر اساس مصرف، منجر به درآمد سالانه حدود ۳.۶ میلیون یورو.
- درآمدهای حاصل از خدمات ارزش‌افزوده امنیتی و پشتیبان‌گیری: پیش‌بینی ارائه خدمات SECaaS و Backup/DR به ۱۰۰ مشتری با میانگین قرارداد سالانه ۵,۰۰۰ یورو، منجر به درآمد سالانه حدود ۰.۵ میلیون یورو.

- درآمدهای حاصل از خدمات مشاوره و ممیزی تخصصی: پیش‌بینی ارائه خدمات به ۵۰ مشتری شرکتی با میانگین پروژه ۱۰,۰۰۰ یورو، منجر به درآمد سالانه حدود ۰.۵ میلیون یورو.
- درآمدهای حاصل از پهنای باند اضافی و خدمات شبکه تخصصی: پیش‌بینی درآمد سالانه حدود ۰.۸ میلیون یورو از مشتریان با نیازهای ترافیکی بالا.

جمع کل درآمدهای پیش‌بینی شده سالانه در وضعیت بهره‌برداری کامل (سال سوم به بعد): حدود ۱۰.۷۸ میلیون یورو

۲. شاخص‌های سودآوری و بازدهی سرمایه‌گذاری:

- سود عملیاتی سالانه (درآمد منهای هزینه عملیاتی): پیش‌بینی حدود ۳.۳۸ میلیون یورو در سال سوم بهره‌برداری کامل.
- دوره بازگشت سرمایه (Payback Period): با در نظر گیری فازبندی سرمایه‌گذاری و تحقق تدریجی درآمدها، پیش‌بینی بازگشت کل سرمایه اولیه ۴۵ میلیون یورو در بازه زمانی ۶ تا ۷ سال از تاریخ شروع فاز اجرایی.
- نرخ بازده داخلی (Internal Rate of Return - IRR): پیش‌بینی IRR پروژه در افق ۱۲ ساله بین ۱۸٪ تا ۲۴٪ با در نظر گیری سناریوهای محافظه کارانه، محتمل و خوش بینانه.
- نسبت سود به هزینه (Benefit-Cost Ratio - BCR): پیش‌بینی BCR پروژه در افق ۱۲ ساله حدود ۲.۸ به ۱ که نشان‌دهنده توجیه اقتصادی قوی طرح است.
- ارزش خالص فعلی (Net Present Value - NPV): با نرخ تنزیل ۱۴٪ (منعکس کننده ریسک بخش فناوری اطلاعات و شرایط منطقه‌ای)، پیش‌بینی NPV مثبت حدود ۲۲ تا ۳۵ میلیون یورو در افق ۱۲ ساله.

۳. شاخص‌های اقتصادی کلان و اثرات سرریز:

- ایجاد اشتغال مستقیم و غیرمستقیم: پیش‌بینی ایجاد ۱۲۰ شغل مستقیم با کیفیت بالا و ۴۰۰ شغل غیرمستقیم در اکوسیستم دیجیتال منطقه در افق ۱۰ ساله.
- جذب سرمایه‌گذاری خارجی تکمیلی: پیش‌بینی جذب حداقل ۶۰ میلیون یورو سرمایه‌گذاری خارجی اضافی از طریق مشتریان بین‌المللی و همکاری‌های استراتژیک با ارائه‌دهندگان خدمات ابری جهانی.
- افزایش صادرات خدمات دیجیتال: پیش‌بینی افزایش صادرات خدمات زیرساختی و ابری ایران به میزان ۱۵ میلیون یورو سالانه در افق ۱۰ ساله به بازارهای منطقه‌ای.
- اثرات فناورانه و دانشی: توسعه دانش بومی در حوزه مدیریت دیتاستر، بهینه‌سازی انرژی و امنیت سایبری، و ایجاد ظرفیت آموزشی برای نیروی انسانی متخصص کشور.

د) مکانیزم‌های پوشش ریسک مالی و تضمین بازدهی:

۱. مکانیزم‌های پوشش ریسک ارزی و هزینه انرژی:

- ایجاد مکانیزم تعدیل تعرفه خدمات بر اساس شاخص‌های تورم بین‌المللی و نوسانات نرخ ارز در قراردادهای بلندمدت با مشتریان استراتژیک، برای حفظ حاشیه سود در شرایط نوسانات اقتصادی.
- تنوع بخشی به سبد ارزی درآمدها با جذب مشتریان بین‌المللی و دریافت پرداخت‌ها به ارزهای مختلف (یورو، دلار، درهم)، همراه با مدیریت هوشمند ریسک ارزی از طریق ابزارهای مالی مجاز.
- سرمایه‌گذاری در سیستم‌های تولید انرژی خورشیدی با ظرفیت حداقل ۵۰۰ کیلووات برای کاهش وابستگی به شبکه سراسری و مدیریت ریسک افزایش قیمت برق در بلندمدت.
- انعقاد قراردادهای تأمین سوخت بلندمدت با پالایشگاه‌های داخلی برای ژنراتورهای اضطراری با قیمت ثابت یا فرمول تعدیل شفاف.

۲. مکانیزم‌های تضمین بازدهی برای سرمایه‌گذاران:

- ساختار حقوقی ترکیبی پروژه با امکان انتشار اوراق مشارکت پروژه محور با سود ثابت سالانه (مثلاً ۱۲٪) برای سرمایه‌گذاران محتاط‌تر، همراه با سهام ممتاز با حق تقدم در توزیع سود برای سرمایه‌گذاران استراتژیک.
- مکانیزم توزیع سود پلکانی که در آن ابتدا هزینه‌های عملیاتی و بازپرداخت تعهدات مالی اولویت‌دار پوشش داده شده، سپس سود حداقلی تضمین شده به سرمایه‌گذاران پرداخت می‌گردد، و مازاد سود طبق درصد توافق شده توزیع می‌شود.
- ایجاد صندوق ذخیره نوسانات (Volatility Reserve Fund) با کسر ۵٪ از سود سالانه برای پوشش دوره‌های رکود موقت بازار یا افزایش غیرمترقبه هزینه‌ها و هموارسازی بازدهی در طول چرخه سرمایه‌گذاری.
- ارائه گزینه خرید سهام توسط منطقه آزاد یا نهادهای همکار پس از دوره قفل‌شدگی ۵ ساله با قیمت مبتنی بر ارزش‌گذاری کارشناسی مستقل، برای ایجاد نقدشوندگی و اطمینان خروج برای سرمایه‌گذاران.

۳. مکانیزم‌های مدیریت ریسک عملیاتی و فنی:

- خرید بیمه‌نامه‌های تخصصی جامع شامل بیمه تمام‌خطر تجهیزات الکترونیکی، بیمه توقف کسب‌وکار (Business Interruption) با پوشش خسارت ناشی از قطعی خدمات، و بیمه مسئولیت حرفه‌ای در قبال مشتریان.
- استقرار سیستم مدیریت ریسک یکپارچه (ERM) مبتنی بر استاندارد ISO 31000 با پایش بلادرنگ شاخص‌های ریسک کلیدی (KRIs) شامل دسترسی پذیری خدمات، مصرف انرژی، رضایت مشتریان، و تهدیدات امنیتی.
- ایجاد کمیته ریسک فنی مستقل در ساختار حاکمیتی دیتاستر با اختیارات نظارتی و تصمیم‌گیری در مورد محدودسازی فعالیت‌های پرریسک، تعلیق موقت خدمات در شرایط بحرانی، و سرمایه‌گذاری در ارتقای تاب‌آوری زیرساخت.
- طراحی و اجرای دوره‌ای سناریوهای استرس‌تست (Stress Testing) برای سنجش تاب‌آوری فنی و مالی دیتاستر در برابر شوک‌های شدید مانند قطع طولانی مدت برق، حملات سایبری گسترده، یا افزایش ناگهانی تقاضا.

بخش دوازدهم: مدت پیشنهادی اجرای طرح با برنامه‌ریزی فازبندی‌شده، مدیریت مسیر بحرانی و دروازه‌های نظارتی

در این برنامه، رویکرد «توازی هوشمند فرآیندها»، «ذخیره‌های زمانی استراتژیک»، و «کنترل کیفیت مرحله‌ای» جایگزین مدل‌های خطی سنتی شده است.

الف) برنامه زمانی فازبندی‌شده دقیق اجرای طرح (مدت کل: ۴۸ ماه تا بهره‌برداری تجاری کامل):

فاز صفر: مطالعات تفصیلی، اخذ مجوزهای حاکمیتی، و آماده‌سازی قراردادی (ماه‌های ۱ تا ۸)

- ماه‌های ۱ و ۲: تشکیل دفتر مدیریت پروژه (PMO) تخصصی، تدوین منشور پروژه (Project Charter) با تعریف دقیق حدود کار، ساختار شکست کار (WBS) در ۵ سطح، و تخصیص منابع انسانی کلیدی. آغاز مطالعات ژئوتکنیک، هیدرولوژی و ارزیابی اثرات زیست‌محیطی (EIA) توسط مشاوران ذی‌صلاح.
- ماه‌های ۳ و ۴: تکمیل طراحی مفهومی و پایه (Conceptual & Basic Design) دیتاستر شامل معماری، سازه، تأسیسات مکانیکی و الکتریکی، و شبکه زیرساخت. همزمان، آغاز فرآیند اخذ موافقت اصولی از سازمان مناطق آزاد، استعلام از سازمان تنظیم مقررات و ارتباطات رادیویی، و آغاز مکاتبات با مرکز افتا برای دریافت پیش‌نیازهای امنیتی.
- ماه‌های ۵ و ۶: تکمیل طراحی تفصیلی (Detailed Design) و تهیه اسناد مناقصه بین‌المللی برای پیمانکاران اصلی (EPC)، تأمین کنندگان تجهیزات حیاتی، و مشاوران ناظر. برگزاری جلسات توجیهی با سرمایه‌گذاران بالقوه و نهادهای مالی برای نهایی‌سازی ساختار تأمین مالی.
- ماه‌های ۷ و ۸: انتخاب پیمانکار EPC و مشاوران ناظر از طریق مناقصه شفاف، انعقاد قراردادهای اصلی، و اخذ مجوزهای نهایی ساخت از مراجع ذی‌صلاح محلی و ملی. آماده‌سازی سایت، تسطیح زمین، و آغاز عملیات خاکی اولیه.

فاز یک: عملیات عمرانی، احداث سازه و تأسیسات پایه (ماه‌های ۹ تا ۲۲)

- ماه‌های ۹ تا ۱۱: اجرای فونداسیون، اسکلت بتنی مسلح، و سقف‌های طبقه اول و دوم دیتاستر. همزمان، اجرای کانال‌های زیرزمینی کابل، مسیرهای تأسیسات، و سیستم زمین‌کردن اصلی.
- ماه‌های ۱۲ تا ۱۴: تکمیل اسکلت، اجرای نازک‌کاری تخصصی شامل کف کاذب ضدلرزه، دیوارهای عایق و ضدگردوغبار، و عایق‌بندی حرارتی-صوتی. آغاز عملیات نصب سیستم‌های توزیع برق اولیه و لوله‌کشی تأسیسات مکانیکی.
- ماه‌های ۱۵ تا ۱۸: تکمیل نمای خارجی، نصب درهای ضدحریق و سیستم‌های کنترل دسترسی اولیه، و راه‌اندازی موقت برق و آب کارگاهی. آغاز تست‌های فشار و نشتی سیستم‌های تأسیساتی.
- ماه‌های ۱۹ تا ۲۲: تکمیل کامل عملیات ساختمانی، اجرای کف‌سازی نهایی سالن‌های سرور، نصب سیستم‌های اعلام و اطفاء حریق، و تحویل موقت ساختمان به پیمانکاران تجهیزات برای آغاز فاز تجهیز. انجام بازرسی‌های سازه‌ای و تأسیساتی توسط دستگاه ناظر و اخذ تأییدیه‌های ایمنی.

فاز دو: تجهیز فنی، نصب زیرساخت‌های حیاتی، و یکپارچه‌سازی سیستم‌ها (ماه‌های ۲۳ تا ۳۲)

- ماه‌های ۲۳ تا ۲۶: ورود و انبارش تجهیزات حیاتی شامل ترانسفورماتورها، ژنراتورها، سیستم‌های UPS، واحدهای خنک‌کننده دقیق (CRAH/CRAC)، و تجهیزات شبکه هسته. آغاز نصب فیزیکی و کابل‌کشی ساختاریافته فیبر نوری و مسی.

- ماه‌های ۲۷ تا ۲۹: راه‌اندازی و تست سیستم‌های توزیع برق، ژنراتورها، و UPS تحت بار مصنوعی. نصب و پیکربندی اولیه سرورها، سیستم‌های ذخیره‌سازی، و پلتفرم‌های مجازی‌سازی. اتصال به شبکه فیبر نوری بین‌المللی و داخلی.
- ماه‌های ۳۰ تا ۳۲: یکپارچه‌سازی نرم‌افزاری سیستم‌های DCIM، SIEM، ITSM و پلتفرم‌های ابری. اجرای تست‌های عملکردی جامع (FAT/SAT)، شبیه‌سازی شرایط قطع برق، بار حرارتی اوج، و حملات سایبری کنترل‌شده. بهینه‌سازی پارامترهای خنک‌کنندگی برای دستیابی به PUE هدف.

فاز سه: راه‌اندازی تجاری، اخذ گواهینامه‌ها، و جذب مشتریان پایه (ماه‌های ۳۳ تا ۳۸)

- ماه‌های ۳۳ تا ۳۵: آغاز بهره‌برداری آزمایشی (Pilot Operation) با حضور تیم‌های فنی و مشتریان منتخب اولیه. ممیزی نهایی توسط سازمان‌های گواهینامه‌دهنده بین‌المللی برای اخذ گواهینامه‌های ISO 27001، ISO 20000، و تأییدیه گرید Tier III از Uptime Institute یا معادل معتبر.
- ماه‌های ۳۶ تا ۳۸: راه‌اندازی رسمی تجاری، فعال‌سازی کامل پورتال مشتری، و آغاز ارائه خدمات IaaS/PaaS/Colocation به بازار. اجرای کمپین‌های بازاریابی تخصصی و امضای قراردادهای بلندمدت با مشتریان استراتژیک (Anchor Tenants).

فاز چهار: بهره‌برداری کامل، توسعه خدمات ارزش افزوده، و پایش عملکرد (ماه‌های ۳۹ تا ۴۸ و پس از آن)

- ماه‌های ۳۹ تا ۴۲: دستیابی به ضریب اشغال ۵۰٪ ظرفیت، پایداری کامل شاخص‌های فنی، و بهینه‌سازی فرآیندهای عملیاتی بر اساس بازخورد مشتریان.
- ماه‌های ۴۳ تا ۴۸: توسعه خدمات امنیتی پیشرفته (SECaaS)، بازیابی فاجعه (DRaaS)، و همکاری‌های بین‌المللی. ارزیابی عملکرد سال اول، بازنگری استراتژیک، و برنامه‌ریزی برای فاز توسعه ظرفیت یا ارتقا به Tier IV.

ب) مدیریت مسیر بحرانی (Critical Path Management - CPM): مسیر بحرانی این پروژه شامل زنجیره‌ای از فعالیت‌های وابسته است که هرگونه تأخیر در آن‌ها مستقیماً تاریخ تحویل نهایی پروژه را به تعویق می‌اندازد. بر اساس تحلیل شبکه‌ای و نرم‌افزارهای مدیریت پروژه پیشرفته، مسیر بحرانی اصلی عبارت است از: اخذ مجوزهای حاکمیتی و محیط‌زیستی ← طراحی تفصیلی و مناقصه EPC ← عملیات خاکی و اسکلت بتنی ← تأمین و واردات تجهیزات حیاتی مثل ترانس، ژنراتور، CRAH، سونچ‌های هسته ← نصب و یکپارچه‌سازی تأسیسات ← تست‌های عملکردی و اخذ گواهینامه.

برای مدیریت بهینه این مسیر، استراتژی‌های ذیل پیاده‌سازی می‌شود:

- موازی‌سازی هوشمند فرآیندها: به‌جای رویکرد ترتیبی، فرآیند طراحی تفصیلی و آماده‌سازی اسناد مناقصه همزمان با اخذ مجوزهای اولیه آغاز می‌گردد. همچنین، فرآیند تأمین تجهیزات حیاتی بلافاصله پس از امضای قرارداد EPC و پیش از

تکمیل ساختمان کلید می خورد تا زمان تحویل تجهیزات (که معمولاً ۶ تا ۹ ماه به طول می انجامد) با عملیات عمرانی همپوشانی داشته باشد.

- ذخیره های زمانی استراتژیک (Time Buffers): به جای اعمال ضریب کلی تأخیر، ذخیره های زمانی هدفمند Project Buffer و Feeding Buffer در انتهای مسیر بحرانی و نقاط اتصال فعالیت های غیر بحرانی به مسیر بحرانی تعبیه می گردد. این ذخیره ها به صورت پویا و بر اساس نرخ مصرف واقعی (Buffer Burn Rate) پایش می شوند.
- مدیریت زنجیره تأمین و لجستیک گمرکی: با استفاده از مزیت های منطقه آزاد، فرآیند ترخیص تجهیزات حیاتی از طریق گمرک اختصاصی فرودگاه و با هماهنگی پیش از ورود با سازمان های ذی ربط انجام می شود. همچنین، قراردادهای تأمین با قیدهای جریمه تأخیر (Liquidated Damages) و ضمانت نامه های پیش پرداخت همراه است.
- پایش هفتگی و اصلاح مسیر: سیستم کنترل پروژه مبتنی بر ارزش کسب شده (EVM) به صورت هفتگی شاخص های SPI و CPI را محاسبه می کند. در صورت انحراف بیش از ۵٪ از برنامه پایه، مکانیزم تصحیح سریع Fast-Tracking یا Crashing با تأیید کمیته راهبری فعال می گردد.

ج) دروازه های نظارتی (Stage-Gate) و معیارهای عبور: هر فاز پروژه مشروط به عبور موفق از دروازه نظارتی مربوطه است که توسط هیئت ممیزی مستقل متشکل از نمایندگان سازمان مناطق آزاد، مشاوران بین المللی دیتاستر، و کارشناسان مالی بررسی می شود. معیارهای کمی و کیفی هر دروازه به شرح ذیل است:

- دروازه پایان فاز صفر: ارائه تأییدیه کتبی مجوزهای ساخت و محیط زیست، تصویب نهایی بودجه تفصیلی، انعقاد قراردادهای EPC و تأمین مالی، و تأیید طراحی پایه توسط مشاوران مستقل. عدم تحقق هر یک از این موارد، مجوز ورود به فاز یک را سلب می نماید.
- دروازه پایان فاز یک: تحویل موقت ساختمان با تأییدیه استحکام سازه، تکمیل سیستم های ایمنی و اطفاء حریق، صدور گواهی های پایان کار موقت تأسیسات، و تأیید آماده سازی فضای فیزیکی برای نصب تجهیزات. معیار عبور: عدم وجود نواقص ایمنی با درجه ریسک بالا و تکمیل ۱۰۰٪ عملیات عمرانی مندرج در WBS.
- دروازه پایان فاز دو: موفقیت در تست های عملکردی یکپارچه (Integrated Systems Testing) شامل شبیه سازی قطع برق سراسری به مدت ۲ ساعت، بار حرارتی ۱۰۰٪، و حمله سایبری سطح ۳. دستیابی به PUE کمتر از ۱.۵ در شرایط تست، و اخذ تأییدیه اولیه امنیتی از مرکز افتا. معیار عبور: رفع کامل تمامی آسیب پذیری های بحرانی و پایداری ۷۲ ساعته سیستم ها بدون خطای عملیاتی.
- دروازه پایان فاز سه: اخذ گواهینامه های بین المللی نهایی، امضای قراردادهای پایه با حداقل ۳ مشتری استراتژیک، پایداری شاخص $Uptime \geq 99.98\%$ به مدت ۳۰ روز متوالی، و تأییدیه نهایی کمیته راهبری برای بهره برداری تجاری کامل.

د) ساختار حاکمیتی نظارت و سیستم پایش بلادرنگ:

- استقرار دفتر مدیریت پروژه یکپارچه (PMO) با اختیارات نظارتی، مالی و فنی، گزارش‌دهی مستقیم به هیئت‌مدیره منطقه آزاد و کمیته سرمایه‌گذاران. PMO مسئولیت هماهنگی بین پیمانکاران، ناظران، تأمین‌کنندگان و نهادهای حاکمیتی را بر عهده دارد.
- پیاده‌سازی پلتفرم دیجیتال مدیریت پروژه مبتنی بر ابر با قابلیت پایش بلادرنگ پیشرفت فیزیکی، مالی و زمانی، مستندسازی الکترونیکی تغییرات (Change Requests)، و تولید خودکار داشبوردهای مدیریتی برای ذی‌نفعان مختلف.
- برگزاری جلسات ماهانه کمیته راهبری عالی با حضور نمایندگان عالی‌رتبه منطقه آزاد، سرمایه‌گذاران اصلی، و مشاوران بین‌المللی برای بررسی انحرافات، تصویب تغییرات استراتژیک، و تصمیم‌گیری در مورد موارد فورس‌ماژور یا تغییر قوانین حاکم.
- انتشار گزارش‌های فصلی عمومی شفاف (با رعایت محرمانگی تجاری) شامل دستاوردها، چالش‌ها، شاخص‌های کلیدی عملکرد (KPIs)، و برنامه‌های آتی برای افزایش اعتماد سرمایه‌گذاران و جامعه محلی.

بخش سیزدهم: انواع قراردادهای پیشنهادی قابل انجام بین منطقه آزاد شهر فرودگاهی امام خمینی (ره) با سرمایه‌گذاران

چارچوب کلی حقوقی حاکم بر قراردادها: کلیه قراردادهای منعقد شده بین منطقه آزاد شهر فرودگاهی امام خمینی (ره) و سرمایه‌گذاران داخلی یا خارجی، در چارچوب قانون چگونگی اداره مناطق آزاد تجاری-صنعتی جمهوری اسلامی ایران، قانون تشویق و حمایت سرمایه‌گذاری خارجی، آیین‌نامه‌های اجرایی سازمان مناطق آزاد، و مقررات سازمان تنظیم مقررات و ارتباطات رادیویی تنظیم می‌گردد. اصل حاکم بر تمامی قراردادهای «تبادل منافع، شفافیت کامل، و تخصیص بهینه ریسک» است؛ بدین معنا که هر ریسک به طرفی تخصیص می‌یابد که بهترین توانایی پیش‌بینی، مدیریت، کنترل یا بیمه آن را داراست. تمامی قراردادها شامل شروط استاندارد حل و فصل اختلاف از طریق داوری ترکیبی (ترکیبی از داوری داخلی در منطقه آزاد و داوری بین‌المللی تحت قواعد آنستیرال یا اتاق بازرگانی بین‌المللی) خواهند بود تا هم سرعت و هزینه حل اختلاف بهینه گردد و هم اعتبار بین‌المللی آرای داوری تضمین شود. همچنین، شرط «ثبات قوانین» (Stabilization Clause) و «جبران تغییر قانون» (Change of Law Compensation) در قراردادهای بلندمدت زیرساختی گنجانده می‌شود تا سرمایه‌گذاران در برابر تغییرات ناگهانی مقرراتی یا مالیاتی مصون بمانند.

۱. قرارداد ساخت، بهره‌برداری و واگذاری (BOT) یا ساخت، تملک و بهره‌برداری (BOO) برای توسعه زیرساخت دیتاستر:

- **طرفین قرارداد:** سازمان منطقه آزاد شهر فرودگاهی امام خمینی (ره) به‌عنوان اعطاکننده حق امتیاز، ارائه‌دهنده زمین، و تسهیل‌گر حاکمیتی، و کنسرسیوم سرمایه‌گذار (شامل شرکت‌های مهندسی، تأمین‌کنندگان تجهیزات، و بهره‌برداران تخصصی) به‌عنوان مجری و بهره‌بردار.

- **موضوع قرارداد:** طراحی، تأمین مالی، احداث، تجهیز و بهره‌برداری از دیتاسنتر ۴۰۰۰ مترمربعی با استانداردهای Tier III/IV در مدل BOT (مدت بهره‌برداری ۲۰ ساله و سپس انتقال رایگان به منطقه آزاد) یا BOO مالکیت دائمی سرمایه‌گذار با تعهدات خدمات عمومی مستمر.

- **ساختار حقوقی و مالی:** ایجاد شرکت پروژه (SPV) تحت قوانین منطقه آزاد با سهم‌الشرکه مشخص. منطقه آزاد ممکن است به صورت سهامی جزئی (تا ۳۰٪) یا بدون سهام، تنها به عنوان ناظر حاکمیتی و اعطاکننده امتیاز وارد قرارداد شود. تأمین مالی از طریق ترکیب آورده سهامداران، تسهیلات بانکی داخلی/خارجی، و اوراق مشارکت پروژه محور انجام می‌پذیرد.

- **تخصیص ریسک:**

- ریسک‌های سیاسی، تغییر قوانین حاکم، و مصادره: بر عهده منطقه آزاد با ارائه تضمین‌های قانونی مبتنی بر قانون حمایت از سرمایه‌گذاری خارجی و بیمه‌های ریسک سیاسی نهادهای بین‌المللی.

- ریسک‌های ساخت، تأخیر، و فراتر رفتن از بودجه: بر عهده پیمانکار EPC و کنسرسیوم سرمایه‌گذار، با مکانیزم‌های جریمه تأخیر (Liquidated Damages) و ضمانت‌نامه‌های حسن انجام کار.

- ریسک‌های بهره‌برداری، بازار، و جذب مشتری: بر عهده بهره‌بردار، با امکان تعدیل تعرفه‌ها بر اساس شاخص‌های تورم و نرخ ارز در صورت وجود مکانیزم‌های تعدیل شفاف در قرارداد.

- ریسک‌های فناوری و انطباق مقرراتی: بر عهده بهره‌بردار با تعهد به رعایت استانداردهای ISO، TIA-942، و مقررات افتا و سازمان تنظیم مقررات، همراه با جبران خسارت ناشی از عدم انطباق.

- **مدت و مکانیزم خروج:** ۲۰ سال برای BOT با امکان تمدید ۵ ساله، یا نامحدود برای BOO. خروج زودهنگام تنها با تأیید کمیته راهبری و فروش سهم به سرمایه‌گذار جایگزین واجد شرایط امکان‌پذیر است. در مدل BOT، در پایان دوره، دارایی‌ها پس از ارزیابی فنی و مالی، به صورت رایگان و با وضعیت عملیاتی مطلوب به منطقه آزاد منتقل می‌گردد.

۲. قرارداد مشارکت در بهره‌برداری و انتقال فناوری (Joint Venture Technology Transfer & Cloud Services)

- **طرفین قرارداد:** منطقه آزاد یا شرکت بهره‌بردار دیتاسنتر، و شرکت بین‌المللی پیشرو در خدمات ابری، مدیریت دیتاسنتر یا امنیت سایبری.

- **موضوع قرارداد:** ایجاد شرکت مشترک برای ارائه خدمات ابری پیشرفته، انتقال دانش فنی مدیریت دیتاسنترهای مقیاس بزرگ، بومی‌سازی پلتفرم‌های نرم‌افزاری، و توسعه اکوسیستم توسعه‌دهندگان داخلی.

- **ساختار حقوقی و مالکیت فکری:** تشکیل شرکت سهامی خاص در منطقه آزاد با تقسیم سهام متناسب با آورده نقدی و غیرنقدی (دانش فنی، لایسنس، برند). مالکیت فکری توسعه‌یافته مشترک، تحت رژیم «مالکیت مشترک متناسب با سهم مشارکت» یا «مالکیت جداگانه بر اساس حوزه تخصص» تعریف می‌گردد. شرط «آموزش و جانشین‌پروری» برای انتقال تدریجی مهارت‌ها به نیروی انسانی ایرانی به صصراًماً درج می‌شود.

- **تخصیص ریسک:**

- ریسک عملکرد فنی و عدم تحقق SLA: بر عهده شرکت مشترک با مکانیزم‌های جریمه داخلی و بیمه مسئولیت حرفه‌ای.
- ریسک نوسانات بازار و رقابت: مشترک بین طرفین، با تقسیم سود و زیان بر اساس نسبت سهام و مکانیزم‌های تعدیل استراتژیک.
- ریسک نقض مالکیت فکری شخص ثالث یا تحریم‌های فناوری: بر عهده شریک خارجی با تعهد به ارائه راه‌حل‌های جایگزین قانونی و جبران خسارت مستقیم.

- **حاکمیت و نظارت:** تشکیل هیئت مدیره با نمایندگی مساوی، کمیته فنی مشترک برای پایش انتقال فناوری، و گزارش دهی فصلی به نهادهای نظارتی منطقه آزاد. مکانیزم خروج شامل حق خرید سهم شریک (Put/Call Option) پس از ۵ سال با قیمت گذاری مبتنی بر ارزش گذاری کارشناسی مستقل.

۳. قرارداد اجاره بلندمدت فضای دیتاستر و خدمات پایه (Anchor Tenant Colocation & Infrastructure Lease Agreement)

- **طرفین قرارداد:** شرکت بهره‌بردار دیتاستر، و مشتریان استراتژیک بزرگ شامل مؤسسات مالی، شرکت‌های مخابراتی، پلتفرم‌های تجارت الکترونیک یا نهادهای حاکمیتی.
- **موضوع قرارداد:** اجاره فضای رک اختصاصی یا نیمه اختصاصی، تأمین برق و خنک‌کنندگی تضمین شده، پهنای باند اختصاصی، و خدمات پشتیبانی فنی ۷/۲۴ در قالب قراردادهای سطح سرویس (SLA) بلندمدت (۳ تا ۱۰ سال).
- **ساختار مالی و SLA:** تعرفه‌ها بر اساس فضای اشغال شده، مصرف برق (kW)، پهنای باند، و سطح خدمات امنیتی تعیین می‌گردد. SLA شامل تعهدات کمی دسترسی پذیری ($\geq 99.98\%$)، زمان پاسخ به حوادث، جبران خسارت در صورت قطعی (Service Credits)، و گزارش دهی شفاف ماهانه است. امکان تمدید خودکار و حق تقدم در توسعه ظرفیت برای مشتریان بلندمدت تعبیه می‌شود.

- **تخصیص ریسک:**

- ریسک قطع خدمات و نقض SLA: بر عهده بهره‌بردار دیتاستر با مکانیزم جبران مالی شفاف و حق فسخ یک طرفه توسط مشتری در صورت تکرار نقض.
- ریسک تأخیر در پرداخت یا ورشکستگی مشتری: بر عهده مشتری با امکان اخذ ضمانت‌نامه بانکی یا ودیعه نقدی، و حق تعلیق خدمات پس از دوره اخطار.
- ریسک تغییر نیازهای فنی مشتری: با مکانیزم انعطاف پذیری قرارداد (Flex Clause) امکان افزایش یا کاهش ظرفیت با اخطار قبلی و تعدیل تعرفه فراهم می‌گردد.

- **حاکمیت و حل اختلاف:** کمیته مشترک فنی-تجاری برای بررسی گزارش‌های SLA و حل اختلافات عملیاتی، ارجاع موارد حقوقی به داوری تخصصی فناوری اطلاعات، و رعایت کامل مقررات حفاظت از داده و محرمانگی اطلاعات مشتری.

۴. قرارداد همکاری استراتژیک اتصال بین‌المللی و تبادل ترافیک (International Peering & Connectivity Partnership)

- **طرفین قرارداد:** منطقه آزاد یا اپراتور شبکه دیتاسنتر، و اپراتورهای بین‌المللی فیبر نوری، شرکت‌های CDN جهانی، یا مراکز تبادل اینترنتی (IXP) منطقه‌ای.
- **موضوع قرارداد:** ایجاد نقاط اتصال مستقیم (PoP) در دیتاسنتر، تبادل ترافیک داده با شرایط Zero-Rating یا هزینه‌های ترجیحی، همکاری در توسعه مسیرهای کم‌تاخیر به اروپا، خلیج فارس و آسیای مرکزی، و ارائه خدمات Edge Computing مشترک.
- **ساختار حقوقی و فنی:** قرارداد چارچوب (Framework Agreement) با پیوست‌های فنی-تجاری برای هر مسیر یا سرویس خاص. رعایت اصول Net Neutrality، شفافیت در مسیریابی ترافیک، و انطباق با مقررات حاکمیت داده ملی. امکان ایجاد کنسرسیوم‌های موقت برای پروژه‌های زیرساختی مشترک.
- **مدیریت ریسک:**

- ریسک اختلال در مسیرهای بین‌المللی یا قطع کابل‌های زیردریایی: مشترک بین طرفین با مکانیزم‌های مسیریابی جایگزین (Diverse Routing) و تقسیم هزینه بازیابی.
- ریسک تغییر مقررات بین‌المللی یا محدودیت‌های ترافیکی: بر عهده طرفی که ذی‌نفع مستقیم تغییر مقررات است، با شرط تجدید مذاکره منصفانه.
- ریسک امنیت ترافیک و نشت داده: بر عهده ارائه‌دهنده سرویس با تعهد به رمزنگاری انتها به انتها و رعایت استانداردهای امنیتی مشترک.

- **حاکمیت و گزارش‌دهی:** کمیته فنی مشترک برای پایش کیفیت مسیرها، گزارش‌دهی ماهانه ترافیک و تاخیر، و مکانیزم حل اختلاف سریع برای اختلالات شبکه. خروج از قرارداد با اخطار ۶ ماهه و تسویه فنی-مالی کامل امکان‌پذیر است.

۵. قرارداد مدیریت و نگهداری عملیاتی برون‌سپاری شده (Operation & Maintenance Outsourcing Agreement)

- **طرفین قرارداد:** مالک یا بهره‌بردار دیتاسنتر، و شرکت تخصصی مدیریت و نگهداری زیرساخت‌های حیاتی (O&M Contractor).
- **موضوع قرارداد:** واگذاری مسئولیت بهره‌برداری روزانه، نگهداری پیشگیرانه و اصلاحی سیستم‌های برق، خنک‌کنندگی، شبکه، امنیت فیزیکی و سایبری، و مدیریت خدمات مشتری به پیمانکار تخصصی.

• **ساختار مالی و عملکردی:** قرارداد مبتنی بر عملکرد (Performance-Based Contracting) با پرداخت‌های ماهانه مشروط به تحقق KPI های تعریف شده شامل MTBF، MTTR، PUE، رضایت مشتری، و نرخ در دسترس بودن خدمات. امکان پاداش عملکرد برای فراتر رفتن از شاخص‌ها و جریمه برای عدم تحقق آن‌ها.

• **تخصیص ریسک:**

- ریسک خرابی تجهیزات و هزینه‌های تعمیر: بر عهده پیمانکار O&M در چارچوب بودجه مصوب نگهداری، مگر در موارد فرسودگی طبیعی یا نقص طراحی اولیه که بر عهده مالک است.
- ریسک حوادث امنیتی یا سایبری ناشی از قصور پرسنل پیمانکار: بر عهده پیمانکار با تعهد به جبران خسارت مستقیم و پوشش بیمه‌ای.
- ریسک کمبود نیروی انسانی متخصص یا ترک خدمت کلیدی: بر عهده پیمانکار با الزام به ارائه برنامه جانشین‌پروری و تأیید صلاحیت پرسنل کلیدی توسط کارفرما.

• **حاکمیت و نظارت:** استقرار سیستم مانیتورینگ بلادرنگ مشترک، گزارش‌دهی هفتگی عملکرد، بازرسی‌های دوره‌ای ناظر مستقل، و حق فسخ یک‌طرفه کارفرما در صورت تکرار عدم انطباق با SLA یا تخلفات امنیتی. دوره قرارداد ۳ تا ۵ ساله با امکان تمدید مشروط به ارزیابی عملکرد مثبت.

ج) چارچوب‌های حکمرانی قراردادی، حل اختلاف و انعطاف‌پذیری:

• **حاکمیت یکپارچه قراردادها:** ایجاد «واحد مدیریت چرخه حیات قراردادها» در منطقه آزاد با مسئولیت پایش تعهدات، مدیریت تغییرات، و تسهیل ارتباط سازنده بین طرفین. استقرار پلتفرم دیجیتال CLM (Contract Lifecycle Management) برای مستندسازی، هشدار خودکار سررسیدها، و تولید گزارش‌های تحلیلی ریسک.

• **مکانیزم‌های انطباق و گزارش‌دهی:** تعهد کلیه طرفین به رعایت «منشور اخلاقی، شفافیت و انطباق منطقه آزاد» شامل مبارزه با فساد، احترام به حقوق مالکیت فکری، و حفاظت از داده‌ها. الزام به ارائه گزارش‌های فصلی شامل عملکرد مالی، فنی، و مدیریت ریسک، همراه با حق بازرسی و ممیزی مستقل توسط کارفرما یا نهادهای ناظر.

• **انعطاف‌پذیری و بازنگری قراردادی:** درج شرط «بازنگری دوره‌ای» در قراردادهای بلندمدت برای تعدیل شرایط بر اساس تحولات فناوری، مقرراتی یا بازار، با مکانیزم مذاکره حسن‌نیت. پیش‌بینی «شرایط فورس ماژور» جامع که شامل رویدادهای طبیعی، تحریم‌های جدید بین‌المللی، تغییرات اساسی قوانین حاکم، و بحران‌های منطقه‌ای باشد، با مکانیزم تعلیق موقت تعهدات یا بازنگری منصفانه شرایط.

• **حل اختلاف و داوری:** ایجاد «کمیته حل اختلاف سریع» متشکل از کارشناسان بی‌طرف داخلی و بین‌المللی برای رسیدگی به اختلافات عملیاتی کوچک قبل از ارجاع به داوری رسمی. در صورت عدم سازش، ارجاع به داوری تحت قواعد آن‌سیترال یا اتاق بازرگانی بین‌المللی با زبان داوری انگلیسی، محل داوری منطقه آزاد یا مرکز بین‌المللی مورد توافق، و الزام به اجرای رأی بر اساس کنوانسیون نیویورک ۱۹۵۸.

- **تضمین‌های اجرایی و انگیزشی:** استفاده از ضمانت‌نامه‌های بانکی، بیمه‌های عملکرد، و مکانیزم‌های جریمه تأخیر متناسب با خسارت محتمل. طراحی مکانیزم‌های پاداش عملکرد برای تشویق طرفین به فراتر رفتن از حداقل تعهدات، و انتشار «گزاره ارزش شفاف» برای هر نوع قرارداد در پلتفرم سرمایه‌گذاری منطقه جهت افزایش اعتماد و جذب سرمایه‌گذاران آگاه.