Annex 3 - Technical Specifications/

Додаток 3. Технічні вимоги

TECHNICAL REQUIREMENTS
Private Cloud Storage and Infrastructure Services/

ТЕХНІЧНІ ВИМОГИ
Послуги приватного хмарного сховища та інфраструктури

Table 1./ Таблиця 1.

No/ № з/п	Name of purchase/ Найменування закупівлі
1	Data processing services, CPV code DK 021:2015 – 72310000-1 (Private cloud storage and infrastructure services)/ Послуги з обробки даних, код ДК 021-2015 – 72310000-1 (Послуги приватного хмарного сховища та інфраструктури)

Procurement Description: Private cloud storage and infrastructure services are required for hosting the information systems of the SE "Ukrainian National Center for Peacebuilding" (hereinafter – the Customer). The information stored on these servers is classified as restricted information in accordance with the Law of Ukraine "On Information".

Private cloud storage and infrastructure services are provided to host the Customer's existing information systems in the Cloud Data Processing Center (hereinafter – CDPC), with the volume of CDPC computing resources specified in Annex 2.1 to the tender documentation. The procurement of these services is carried out for the Customer's existing information systems, which are developed and operating on the VMware hypervisor software.

If a bidder proposes a solution based on alternative hypervisor software (other than VMware), the bidder must ensure:

- migration and conversion of encrypted virtual machines from the VMware format to another virtualization platform without decrypting the virtual machine. After such migration, the operating system and services inside the encrypted virtual machine must operate without interruption.

- availability of a REST API for automating routine cloud infrastructure management tasks, including:

Integration with Kubernetes clusters, including:

- initializing a node with cloud-specific labels (zones/regions)
- retrieving node IP addresses and hostnames
- removing Kubernetes nodes if they are removed from the cloud
- dynamic creation and management of data storage for containers.

Integration with Terraform, including
- automated creation, modification, and deletion of infrastructure;
- repeated creation of environments with identical parameters to ensure deployment consistency;

Опис закупівлі: Послуги приватного хмарного сховища та інфраструктури необхідні для розміщення потужностей інформаційних систем ДП «Український національний центр розбудови миру» (далі – Замовник). Інформація, яка розміщена на цих серверах, відповідно до Закону України «Про інформацію» відноситься до службової інформації.

Послуги приватного хмарного сховища та інфраструктури надаються для розміщення існуючих інформаційних систем Замовника у Хмарному Центрі Обробки Даних (далі – ХЦОД) з об'ємом споживання обчислювальних ресурсів ХЦОД, зазначених в додатку 2.1.до тендерної документації. Закупівля даних послуг здійснюється для існуючих інформаційних систем Замовника, які розроблені та функціонують на базі ПЗ гіпервізора VMware.

У разі надання пропозиції учасника рішення з використанням альтернативного програмного забезпечення гіпервізора (відмінного від VMware) учасник забезпечує:

- міграцію та конвертацію шифрованих віртуальних машин з формату VMware на іншу платформу віртуалізації без виконання розшифрування віртуальної машини. Після такої міграції, операційна система та сервіси в середині шифрованої віртуальної машини повинні працювати безперебійно.

- наявність REST API для можливості автоматизації рутинних завдань по управлінню хмарною інфраструктурою, а саме:

Інтеграція з кластерами Kubernetes, у тому числі:
- ініціалізація вузла з мітками, специфічними для хмари (зони/регіони).
- отримання IP-адрес та імен хостів вузлів
- видалення Kubernetes вузлів, якщо вони видалені з хмари.
- динамічне створення та управління сховищами даних для контейнерів;

Інтеграція з Terraform, у тому числі
- автоматизоване створення, зміна та видалення інфраструктури;
- багаторазове створення середовищ з аналогічними параметрами для консистентості розгортання;

- a link to the manufacturer's technical documentation for the alternative hypervisor describing the availability of the required functionality;

- availability of a Terraform Provider for the specified REST API. The Terraform Provider for this REST API must have an "Official" or "Partner" status.

A bidder offering an alternative hypervisor must possess the technologies and tools that enable the secure conversion of vmx (virtual machine configuration file) and vmdk (virtual disk file format) into the format of the alternative hypervisor and must be able to apply these tools during the migration of workloads from the Customer's infrastructure to the bidder's cloud at no additional cost to the Customer.

A bidder offering an alternative hypervisor must possess the technologies and tools that enable the use of VXLAN or Geneve in broadcast mode, as required for deploying the Customer's virtual network infrastructure, supporting more than 4096 L2 and L3 virtual networks according to the OSI model, using built-in hypervisor tools and without additional network equipment.

- availability of connectivity to the Secure Internet Access Nodes (ZVID).

An active ZVID contract with Datagroup PJSC, certificate of compliance No. 15595 dated 13.09.2017

In addition to the above requirements, uninterrupted operation of the information system is essential. A fast and seamless transition between providers would additionally require services for the migration and configuration of the network infrastructure and specialized security modules, involving contractors responsible for the development and implementation of protection measures in accordance with the Integrated Information Security System (KSZI/IISS) standards, as well as software developers and the current cloud service provider.

- посилання на технічну документацію виробника альтернативного Гіпервізора з описом наявності вказаної функціональності;

- наявність Terraform Provider для вказаного REST API. Terraform Provider для вказаного REST API повинен мати статус «Official» або «Partner».

Учасник, що пропонує альтернативний гіпервізор, володіє технологіями та інструментами, що дозволяють безпечну конвертацію файлів vmx (конфігураційний файл віртуальної машини) та vmdk (формат файлу віртуального диску) у формат альтернативного гіпервізора, та здатен застосувати їх під час міграції робочих навантажень з власної інфраструктури Замовника у хмару учасника без додаткової оплати з боку Замовника.

Учасник, що пропонує альтернативний гіпервізор, володіє технологіями та інструментами, що дозволяють застосування технологіїї VXLAN або Geneve в броадкаст-режимі, як це потрібно для засобів розгортання віртуальної мережевої інфраструктури Замовника в кількості більше ніж 4096 віртуальних мереж L2 та L3 згідно моделі OSI вбудованими засобами гіпервізора та без застосування додаткового мережевого обладнання.

- наявність можливості підключення до Захищених вузлів доступу до мережі Інтернет (ЗВІД) Діючий договір на ЗВІД з ПрАТ «ДАТАГРУП», атестат відповідності № 15595 від 13.09.2017

Окрім зазначених вимог існує потреба в безперебійній роботі інформаційної системи. Швидкий і безперебійний перехід між провайдерами потребуватиме додатково послуги з міграції та налаштування мережевої інфраструктури та спеціальних модулів безпеки із залученням підрядників, які забезпечували розробку та впровадження захисту згідно норм КСЗІ, розробників ПЗ та поточного провайдера хмарних послуг.

Terms and Definitions:

Data Center (DC) – a specialized technical facility consisting of engineering systems (uninterruptible power supply, ventilation, cooling and humidity control, fire safety, physical security), information, electronic communications, and hardware–software infrastructure whose components provide or enable data storage and processing services, including but not limited to: cloud services, data backup, data transmission, equipment rack rental, and hosting services.

Infrastructure – server hardware, network equipment, and system software.

Cloud Data Center (CDPC) – a cloud infrastructure that logically encompasses a defined set of the Contractor's computing hardware resources, owned, managed, and operated by the Contractor, and intended for hosting the Customer's services. In this setup, servers, network devices, and storage systems are used exclusively for the Customer's services (they do not host services of other clients), have a separate management system, and are located in a dedicated cabinet within the Data Center. The Contractor provides Virtual Private Cloud services using the CDPC computing resources. The CDPC is located in the Contractor's DC(s).

Virtual Private Cloud (VPC) – a logically unified set of virtual computing resources from the CDPC resource pool,

Терміни та визначення:

ЦОД (Центр Обробки Даних**) –** спеціалізований технічний комплекс, що складається з інженерної (системи безперебійного електроживлення, вентиляції, охолодження та регулювання вологості, пожежної безпеки, фізичної охорони), інформаційної, електронної комунікаційної та програмно-апаратної інфраструктури, засоби якого забезпечують або реалізують надання послуг із зберігання та обробки даних, у тому числі, але не обмежуючи: надання хмарних послуг, резервного копіювання даних, передачі даних, оренди комунікаційних стійок, послуг хостингу.

Інфраструктура – серверне обладнання, мережеве обладнання та системне програмне забезпечення.

ХЦОД (Хмарний Центр Обробки Даних) – це хмарна інфраструктура, що на логічному рівні охоплює певний набір апаратних обчислювальних ресурсів Виконавця, яка є у володінні, керуванні та експлуатації Виконавця та призначені для розміщення сервісів Замовника. При цьому сервери, мережні пристрої та сховища використовуються виключно для розміщення сервісів Замовника (не містять сервісів інших клієнтів Виконавця), мають відокремлену систему управління та розміщені у Дата-центрі у окремій апаратній шафі. Виконавець надає послугу Віртуальної приватної хмари використовуючи обчислювальні ресурси ХЦОД. ХЦОД розміщується у ЦОД(ах) Виконавця.

Віртуальна приватна хмара (VPC) – є доступним на вимогу Замовника об'єднаним на логічному рівні

provided to the Customer on demand and intended exclusively for the Customer's use.

Secure Site – a combination of the Virtual Private Cloud and additional computing and network equipment used by the Customer.

Hypervisor (or Virtual Machine Monitor) – software or hardware that enables simultaneous, parallel execution of multiple operating systems on the same computer (the host computer), providing OS isolation, resource separation among running OSs, and resource management

Virtual Machine (VM) – a model of a computing system created through virtualization of resources such as CPU, RAM, storage devices, and input/output devices. Unlike software that emulates a specific device, a VM provides full emulation of a physical machine or runtime environment.

Operating System (OS) – a basic software environment that manages the hardware of a computer or virtual machine, controls computing processes, and organizes interaction with the user.

Hard Disk (HDD) – a magnetic disk drive with a rigid substrate.

Virtual Disk – software components that emulate physical disk storage devices and attach to virtual machines. The virtual disk must be recognized by the OS as a hard disk.

Cloud Storage – a data storage model where digital data is stored in logical pools, while physical storage spans multiple servers and disk systems. The physical environment is owned and managed by the Contractor.

Virtual Core – a CPU core emulated by the hypervisor for the operating system. The hypervisor may manage the computing performance of the virtual core.

RAM (Random Access Memory) – memory used by computing systems to store program code and data during execution.

MB (Megabyte) – a unit of data equal to 1,048,576 (2^{20}) bytes or 1024 kilobytes.
GB (Gigabyte) – a multiple unit of information measurement equal to 1,073,741,824 (2^{30}) standard 8-bit bytes or 1024 megabytes.
TB (Terabyte) – a unit of data equal to 1,099,511,627,776 (2^{40}) standard 8-bit bytes or 1024 gigabytes.

Mbit/s (Megabit per second) – a data transfer rate equal to 1,000,000 bits per second.
Gbit/s (Gigabit per second) – a data transfer rate equal to 1,000,000,000 bits per second.
RFC (Request for Comments) – a numbered series of Internet technical documents containing specifications and standards, widely used across the global network. RFCs are published by the IETF under the Internet Society (ISOC), https://www.ietf.org/).

набором віртуальних обчислювальних ресурсів Виконавця з пулу ресурсів ХЦОД та призначені для надання послуг виключно Замовнику.
Захищений майданчик – об'єднує у собі Віртуальну приватну хмару та додаткове обчислювальне та мережеве обладнання, що використовуються Замовником.
Гіпервізор (або Монітор віртуальних машин) – комп'ютерна програма або обладнання, що забезпечує одночасне, паралельне виконання декількох операційних систем на одному і тому ж комп'ютері (який тоді зветься хост-комп'ютер англ. host computer). Гіпервізор також забезпечує ізоляцію операційних систем одну від одної, розділення ресурсів між різними запущеними ОС і керування ресурсами.
Віртуальна машина (VM/ВМ) – модель обчислювальної машини, створеної шляхом віртуалізації обчислювальних ресурсів: процесора, оперативної пам'яті, пристроїв зберігання та вводу і виводу інформації. Віртуальна машина, на відміну від програми емуляції конкретного пристрою, забезпечує повну емуляцію фізичної машини чи середовища виконання (для програми).
Операційна система (скорочено ОС, англ. Operating system, OS) – це базовий комплекс програмного забезпечення, що виконує управління апаратним забезпеченням комп'ютера або віртуальної машини; забезпечує керування обчислювальним процесом і організовує взаємодію з користувачем.
Твердий диск (або Накопичувач на магнітних дисках (англ. Hard (magnetic) disk drive, англ. HDD)) – магнітний диск, основа якого виконана з твердого матеріалу.
Віртуальний диск – програмні компоненти, які емулюють роботу фізичних дискових накопичувачів інформації, та підключаються до віртуальних машин. Віртуальний диск має сприйматися Операційною системою, як твердий диск.
Хмарне сховище – являє собою модель зберігання даних, де цифрові дані зберігаються в логічному пули, а фізичне зберігання охоплює кілька серверів та дискових систем. Фізичне середовище при цьому, належить і керується Виконавцем.
Віртуальне ядро – емуляція гіпервізором звичайного ядра для операційної системи. Гіпервізор при цьому може управляти обчислювальною продуктивністю Віртуального ядра.

Оперативна пам'ять (англ. Random Access Memory) – пам'ять обчислювальних машин призначена для зберігання коду та даних програм під час їхнього виконання.

МБ (Мегабайт) – одиниця виміру обсягу даних. Дорівнює 1 048 576 (2^{20}) байт або 1024 кілобайт.
ГБ (Гігабайт) – кратна одиниця виміру кількості інформації, що дорівнює 1 073 741 824 (2^{30}) стандартним (8-бітним) байтам або 1024 мегабайтам.
ТБ (Терабайт) – кратна одиниця виміру кількості інформації, що дорівнює (2^{40} = 1 099 511 627 776) стандартним (8-бітним) байтам або 1024 гігабайтам.
Мбіт/с (Мегабіт в секунду) – одиниця швидкості передачі даних, що дорівнює передачі 1 000 000 біт у секунду.
Гбіт/с (Гігабіт в секунду) – одиниця швидкості передачі даних, що дорівнює передачі 1 000 000 000 біт у секунду.
RFC (англ. Request for Comments, Запит коментарів) – документ із серії пронумерованих інформаційних документів Інтернету, що містить технічні специфікації та Стандарти, має широке застосування у всесвітній мережі. Зараз публікацією документів RFC займається

IETF під егідою відкритої організації Товариство Інтернету (англ. Internet Society, ISOC, https://www.ietf.org/).

IP Address – a unique numerical identifier at the network layer used for addressing computers and devices in networks based on TCP/IP (including the Internet).

IP адреса (англ. Internet Protocol address) – це ідентифікатор (унікальний числовий номер) мережевого рівня, який використовується для адресації комп'ютерів чи пристроїв у мережах, які побудовані з використанням протоколу TCP/IP (наприклад Інтернет).

IPv4 (Internet Protocol version 4) – the fourth version of the IP network protocol, defined in RFC 791.

IPv4 (англ. Internet Protocolversion 4) – четверта версія мережевого протоколу IP. Протокол IPv4, описаний у RFC 791.

Host – any computing device with access to an IP network; synonymous with a network node.

Хóст - будь який комп'ютерний пристрій, що має доступ до IP мережі тобто синонім терміну вузол мережі.

FTT (Failures to Tolerate) – the number of simultaneous vSAN cluster node failures the system can withstand without data loss.

FTT (англ. Failures to Tolerate) – кількість одночасних відмов нод кластеру vSAN, який не призводить до втрати даних.

VLAN (Virtual Local Area Network) – a group of hosts with common requirements that interact as if connected to the same domain, regardless of physical location. VLANs share attributes of physical LANs but allow grouping of endpoints even when not on the same switch.

VLAN (англ. Virtual Local Area Network – віртуальна локальна комп'ютерна мережа) – є групою Хостів з загальним набором вимог, що взаємодіють так, ніби вони прикріплені до одного домену, незалежно від їх фізичного розташування. VLAN має ті самі атрибути, як і фізична локальна мережа, але дозволяє кінцевим станціям бути згрупованими разом, навіть якщо вони не перебувають на одному мережевому комутаторі.

iSCSI (Internet Small Computer System Interface) – a protocol based on TCP/IP used to establish interaction and management of storage systems, servers, and clients. iSCSI is standardized in RFC 3721, RFC 3722, RFC 3723, RFC 3347, RFC 3783, RFC 3980, RFC 4018, RFC 4173, RFC 4544, RFC 4850, RFC 4939, RFC 5048, RFC 5047, RFC 5046, and RFC 7143.

iSCSI (англ. Internet Small Computer System Interface) – протокол, який базується на TCP/IP і розроблений для встановлення взаємодії та управління системами зберігання даних, серверами і клієнтами. Протокол iSCSI є стандартизованим в RFC 3721, RFC 3722, RFC 3723, RFC 3347, RFC 3783, RFC 3980, RFC 4018, RFC 4173, RFC 4544, RFC 4850, RFC 4939, RFC 5048, RFC 5047, RFC 5046 і RFC 7143.

NFS (Network File System) – a network file access protocol originally developed by Sun Microsystems in 1984, allowing remote file systems to be mounted over a network; described in RFC 1094, RFC 1813, RFC 3530, and RFC 5661.

NFS (Network File System) – протокол мережевого доступу до файлових систем, спочатку розроблений Sun Microsystems в 1984 році. Дозволяє підключати (монтувати) віддалені файлові системи через мережу, описаний в RFC 1094, RFC 1813, RFC 3530 і RFC 5661.

SMB (Server Message Block) – an application-layer protocol used for shared access to files, printers, serial ports, and other interactions between nodes. It also provides interprocess communication with authentication. Commonly used in Microsoft Windows environments (“Microsoft Windows Network”).

SMB (англ. Server Message Block) – протокол прикладного рівня (в моделі взаємодії відкритих систем), використовується для надання розділеного доступу до файлів, принтерів, послідовних портів передачі даних, та іншої взаємодії між вузлами в комп'ютерній мережі. Також надає можливості міжпроцесної взаємодії з автентифікацією. Зазвичай, використовується на комп'ютерах з Microsoft Windows: в середовищі Microsoft, часто позначається як «Microsoft Windows Network»

Data Integrity – a condition ensuring that data has not been altered during operations such as transmission, storage, or display.

Цілісність інформації (англ. data integrity, information integrity) – термін, який вказує, що дані не були змінені при виконанні будь-якої операції над ними, будь то передача, зберігання і відображення.

Integrity of Information System Resources – a condition where changes to system resources are made only intentionally by authorized subjects, while preserving their composition, structure, and interactions.

Цілісність ресурсів інформаційної системи – стан ресурсів інформаційної системи, при якому їх зміна здійснюється тільки навмисно суб'єктами, що мають на це право, при цьому зберігаються їх склад, зміст та організація взаємодії.

SLA (Service Level Agreement) – an appendix to the main agreement between the Contractor and Customer defining quantitative and qualitative characteristics of services, such as availability, user support, and time to resolve incidents.

SLA (англ. Service Level Agreement, Угода про рівень обслуговування) – додаток до основної угоди між Виконавцем та Замовником про рівень послуг. Містить кількісні та якісні характеристики наданих послуг, такі як їх доступність, підтримка користувачів з боку Замовника, час виправлення несправності та інше.

IOPS (Input/Output Operations Per Second) – the standard metric of performance for computer storage systems such as hard drives and other storage devices.

IOPS (англ. Input-Output Operations Per Second) – кількість операцій вводу/виводу, стандартний вимір продуктивності комп’ютерних систем зберігання даних таких як тверді диски та інші пристрої зберігання даних.

Ethernet – a fundamental technology for local computing (computer) networks with packet switching that uses the

Ethernet – базова технологія локальних обчислювальних (комп'ютерних) мереж з комутацією пакетів, що використовує протокол CSMA/CD

CSMA/CD protocol (carrier-sense multiple access with collision detection).

IEEE (Institute of Electrical and Electronics Engineers) – an international organization of engineers in electrical engineering, electronics, and related industries.

SFP+ (Enhanced SFP) – a data transmission interface supporting speeds up to 10 Gbit/s, specified in SFF-8418 (http://www.sffcommittee.com/).
Edge Router – a router located at the external perimeter of the Contractor's CDPC.

DNAT (Destination Network Address Translation) – translation of the destination network address.
SNAT – (Source Network Address Translation) – translation of the source network address.
ACL (Access Control List) – a list of permissions defining who or what may access an object and which operations are allowed or denied.

BGP – (Border Gateway Protocol) – the standard inter-domain routing protocol used between autonomous systems on the global Internet.

Business Hours – 08:00 to 19:00 on working days.
Incident – an event resulting in partial or complete deviation of service quality from the nominal level.
KZZ – security measures suite.

Requirements for the Technical and Quality Characteristics of the Services

1. General Description of the Services

Within the Private Cloud Storage and Infrastructure Service, the Customer receives access to the computing resources of a Virtual Private Cloud.
A non-exhaustive list of **VPC** operations available to the Customer within the Virtual Private Cloud service:

1.1. Create or delete virtual machines and modify their configuration.
1.2. Power on and power off virtual machines; access their consoles.
1.3. Create, delete, configure, and attach virtual disks and Private Cloud Storage resources to virtual machines.
1.4. Manage network configuration and connect or disconnect virtual machines from the network.
1.5. Create, delete, and configure virtual networks.
1.6. Configure routing rules of the router connected to the Internet.
1.7. Install system and application software on virtual machines and manage it.

2. Core Technical Requirements for the VPC

2.1. The Contractor shall provide the Customer with the resources listed in Annex 2.1 to the tender documentation.
2.2. The volume of VPC resources provided from the CDPC resource pool must include redundancy of all components of the complex in an amount sufficient to maintain its proper functioning even in the event of failure of any hardware component.

(множинний доступ з контролем несучої та виявленням колізій).

IEEE (англ. Institute of Electrical and Electronics Engineers, Інститут інженерів з електротехніки та електроніки) – міжнародна організація інженерів у галузі електротехніки, радіоелектроніки та радіоелектронної промисловості.
SFP+ (англ. Enhanced SFP) – інтерфейс передачі даних до 10 Гбіт/с, параметри якого визначені у специфікації SFF-8418 (http://www.sffcommittee.com/).
Граничний маршрутизатор (англ. Edge router) – маршрутизатор, який розташований на зовнішньому периметрі ХЦОД Виконавця.
DNAT – (англ. Destination Network Address Translation) – Зміна Мережевої Адреси Отримувача.
SNAT – (англ. Source Network Address Translation) – Зміна Мережевої Адреси Відправника.
ACL (англ. Access Control List, список контролю доступу) – список прав доступу до об'єкта, який визначає, хто або що може отримувати доступ до нього, і які саме операції дозволено або заборонено цьому суб'єкту проводити над об'єктом.
BGP – (англ. Border Gateway Protocol, Протокол Граничного Шлюзу) – єдиний протокол маршрутизації між автономними системами в глобальній мережі Інтернет.
Бізнес-час - години з 8:00 до 19:00 у робочі дні.
Інцидент – подія, що призвела до часткового або повного відхилення якості сервісу від номінального рівня.
КЗЗ – комплекс засобів захисту.

Вимоги до технічних та якісних характеристик Послуг

1. Загальний опис Послуг

В межах Послуги приватного хмарного сховища та інфраструктури Замовник отримує в користування обчислювальні ресурси Віртуальної приватної хмари.
Набір операцій **VPC** (не є вичерпним), які доступні Замовнику в межах послуги Віртуальної приватної хмари:

1.1. Створювати або видаляти віртуальні машини та змінювати їх конфігурацію.
1.2. Вмикати та вимикати віртуальні машини, отримувати доступ до їх консолей.
1.3. Створювати, видаляти, налаштовувати та підключати до віртуальних машин віртуальні диски та ресурси Приватного хмарного сховища.
1.4. Керувати конфігурацією мережі, підключати та відключати від неї віртуальні машини.
1.5. Створювати, видаляти та налаштовувати віртуальні мережі.
1.6. Налаштовувати правила маршрутизації маршрутизатора, що підключений до Інтернет.
1.7. Встановлювати на віртуальні машини системне та прикладне програмне забезпечення та керувати ним.

2. Основні технічні вимоги до VPC

2.1. Виконавець надає у користування Замовнику ресурси, перелік та об'єм яких вказаний в Додатку 2.1 до тендерної документації.
2.2. Об'єм ресурсів VPC, що надається Виконавцем з пулу ресурсів ХЦОД повинен мати резервування всіх компонентів комплексу в кількості, необхідній для підтримки належної працездатності комплексу навіть у випадках відмови будь якої апаратної компоненти.

2.3. Availability of a portal and/or graphical administrator interface that enables the Customer to manage virtual machines created in the Virtual Private Cloud (number of processors/cores, RAM volume, number and size of disks, number of network adapters, type of operating system).

3. Core Technical Requirements for the CDPC

3.1. All hardware resources used to build the CDPC and the Contractor's server cabinets shall be located in Ukraine and within a single site.

3.2. Hardware servers, network equipment, and storage systems used to form the VPC resource pool must not be used to provide services to other clients of the Contractor.

3.3. The Contractor may choose the composition of the CDPC and the configuration of its components at its own discretion, subject to the following limitations:

3.3.1. The composition of the CDPC and the configuration of its components must meet the Customer's need for highly available physical resources specified in the relevant tables. The physical resource volumes listed must be fully available to the Customer even in the event of hardware failures, in accordance with the target redundancy levels.

3.3.2. Target redundancy levels (number of standby components in "hot" reserve mode) must be no lower than: N+1 for servers, N+2 for vSAN disk groups (ensuring data integrity and availability in case of simultaneous failure of **any** two disk groups), N+2 for NL-SAS disks NL-SAS, 2N for other NL-SAS storage components and network equipment.

3.3.3. SSD-type virtual disks must be created using vSAN technology or an equivalent, and must support the use of persistent volumes.

3.3.4. Servers used to create the VPC resource pool must be equipped with processors of the Intel Scalable Xeon 2nd Generation family or higher.

3.3.5. The bandwidth of network adapter ports of computing nodes (servers) and of the switch ports they are connected to must be at least 10 Gbit/s.

3.4. The fault-tolerance SLA for the specific VM must be no less than 99.95% per year.

3.5. It must be possible to implement fault-tolerant Internet access based on an architecture using multiple providers and external addresses routed via the BGP protocol.

3.6. The ability to choose an Internet service provider and/or dedicated communication channels.
If the Internet/dedicated channel provider selected by the Customer does not yet have a direct connection to the Contractor's Data Center, the ability to connect must be provided without restrictions. Work required on the Contractor's side must not exceed 5 working days.

2.3. Наявність порталу та/або графічного інтерфейсу адміністратора, який дозволяє Замовнику управляти віртуальними машинами, що створюються у Віртуальній приватній хмарі (кількість процесорів/ядер, об'єм оперативної пам'яті, кількість та об'єм дисків, кількість мережевих адаптерів, тип операційної системи).

3. Основні технічні вимоги до ХЦОД

3.1. Усі апаратні ресурси, що використовуються для створення ХЦОД, та комп'ютерні шафи Виконавця мають знаходитися на території України і в межах однієї локації.

3.2. Апаратні сервери, мережеве обладнання та системи збереження даних, що задіяні для створення ресурсного пулу VPC, не повинні використовуватися для надання послуг іншим замовникам Виконавця.

3.3. Виконавець може обирати склад ХЦОД та конфігурацію його компонент на власний розсуд з урахування наступних обмежень:

3.3.1. Склад ХЦОД та конфігурація його компонент повинна забезпечувати потреби замовника у високодоступних фізичних ресурсах, що зазначені у відповідних таблицях. Наведений в таблицях об'єм фізичних ресурсів повинен бути доступний Замовнику в повному обсязі навіть у випадках апаратних відмов відповідно до цільових рівнів резервування.

3.3.2. Цільові рівні резервування (кількість резервних компонент у складі комплексу у режимі «гарячого» резерву) повинна бути не нижче ніж: N+1 для серверів, N+2 для дискових груп vSAN (збереження цілісності та доступності даних у випадку одночасного виходу зі строю **будь-яких** двох дискових груп), N+2 для дисків NL-SAS, 2N для інших компонентів СЗД NL-SAS та мережевого обладнання.

3.3.3. Віртуальні диски типу SSD повинні бути створені за допомогою технології vSAN або аналогічні та підтримувати роботу з persistent volumes.

3.3.4. Сервери, що використовуються для створення ресурсного пулу VPC, повинні бути обладнані процесорами сімейства не нижче Intel Scalable Xeon 2-nd Generation.

3.3.5. Пропускна здатність портів мережевих адаптерів обчислювальних вузлів (серверів) та портів мережевих комутаторів, до яких вони підключені, повинна бути не нижче 10 Гбіт/с.

3.4. SLA відмовостійкості конкретної VM повинен бути не менше ніж 99,95% за рік.

3.5. Має бути можливість реалізації відмовостійкого доступу до мережі Інтернет на основі архітектури використання декількох провайдерів та зовнішніх адрес, які маршрутизуються за допомогою протоколу BGP.

3.6. Можливість обирати постачальника послуг Інтернет та/або виділених каналів. Якщо обраний Замовником постачальник послуг Інтернет та/або виділених каналів ще не має прямого підключення до ЦОД Виконавця, то можливість підключитися має бути надана без обмежень. Виконання необхідних на боці Виконавця робіт не має перевищувати 5 робочих діб.

3.7. The Contractor shall ensure and guarantee complete isolation of the Customer's data stored/processed in the Virtual Private Cloud from third parties. Only the Customer shall control access to the data stored in the Virtual Private Cloud.

3.8. If commercial software requiring licensing is used for building the CDPC, the Contractor must hold valid licenses for all commercial CDPC software.

3.9. In the event of a failure of a physical server running a Virtual Machine, the VM must be automatically switched to another physical server, with a switchover time not exceeding 10 minutes (excluding OS and application startup time).

3.10. 24/7 support (24 hours, 7 days a week) via phone and email.

3.11. Availability of spare parts (Spares Kit) to enable rapid restoration of the basic configuration of the complex.

3.12. The Customer must be provided with the ability to manage Cloud Storage via an administrator interface within the allocated resources.

3.13. The Contractor shall ensure the ability to migrate data between storage resources of different performance levels without interruption of service.

4. Requirements for the CDPC Information Security System

General Requirements:

4.1. For all components included in the CDPC, organizational measures, antivirus protection measures, physical security, procedures for creation, implementation, testing, and other related matters shall be addressed within the CDPC as a whole.

4.2. The administrative access control mechanism shall be implemented at the level of access to CDPC resources and the CDPC management system.

4.3. Administration of the Complex of Protection Measures (CPM) shall be carried out only by authorized personnel of the information security unit. Actions involving changes to the configuration or composition of the CPM and the reasons for such actions must be recorded in specifically designated logs.

4.4. The Bidder's cloud infrastructure must be certified for compliance with the requirements of the Integrated Information Security System (KSZI) with the capability of processing restricted information. It must represent a set of hardware and software components deployed at the Bidder's technical site and must comply with the regulatory documents of the Ukrainian Technical Information Protection System. The Bidder's technical site must include components of the Private Cloud Infrastructure.

4.5. The Customer has the right to verify that the CDPC meets the requirements specified in this Annex by using remote access to the VPC in test mode or

3.7. Виконавець забезпечує/гарантує повну ізоляцію даних Замовника, що зберігаються/обробляються у Віртуальній приватній хмарі від третіх осіб. Управляти доступом до даних, що зберігаються у Віртуальній приватній хмарі має лише Замовник.

3.8. В разі використання для створення ХЦОД комерційного програмного забезпечення, що потребує ліцензування, Виконавець повинен мати дійсні ліцензії на все комерційне програмне забезпечення ХЦОД.

3.9. У випадку збою фізичного серверу, на якому була запущена Віртуальна машина, повинно відбуватися автоматичне переключення Віртуальної машини на інший фізичний сервер, при цьому час переключення не має перевищувати 10 хв. (не рахуючи запуск операційної системи та аплікацій)

3.10. Підтримка 24/7 (24 години, 7 днів на тиждень) по телефону та електронною поштою.

3.11. Наявність ЗІП для можливості оперативного відновлення працездатності базової конфігурації комплексу.

3.12. Замовнику має бути надано можливість управляти Хмарним сховищем, використовуючи інтерфейс для адміністратора, у межах заявлених ресурсів.

3.13. Виконавець забезпечує можливість міграції даних між дисковими ресурсами різної продуктивності без переривання в роботі сервісу.

4. Вимоги до системи захисту інформації ХЦОД

Загальні вимоги:

4.1. Для всіх компонентів, що входять до складу ХЦОД, організаційні заходи, заходи антивірусного захисту, фізичної охорони, питання щодо порядку створення, впровадження, проведення випробувань та інші вирішуються в межах ХЦОД в цілому.

4.2. Механізм адміністративного управління доступом реалізується на рівні доступу до ресурсів ХЦОД та системи управління ХЦОД.

4.3. Адміністрування КЗЗ здійснюється лише уповноваженим персоналом служби захисту інформації. Дії зі зміни конфігурації або складу КЗЗ та причини, що їх викликали, повинні відображатись в спеціально визначених журналах.

4.4. Хмарна інфраструктура Учасника, повинна бути атестована на відповідність вимогам Комплексної Системи Захисту Інформації (КСЗІ) з можливістю обробки службової інформації, являти собою сукупність апаратних та програмних компонентів, які розгортаються на технічному майданчику Учасника та повинна задовольняти вимогам нормативних документів системи технічного захисту інформації України. До складу технічного майданчика Учасника повинні входити компоненти Приватної хмарної інфраструктури.

4.5. Замовник має право на перевірку відповідності ХЦОД зазначеним в цьому Додатку вимогам з використанням

directly at the Contractor's site, provided that the Contractor is notified at least 10 working days in advance.

4.6. The CDPC must ensure compliance with the requirements for personal data protection in accordance with the Law of Ukraine "On Personal Data Protection".

The CDPC Information Security System shall ensure:

4.7. Development by responsible personnel of rules for separating user access to CDPC resources (procedures for granting and distributing administrator rights and individual privileges), as well as procedures for monitoring their application;

4.8. Separation of administrator functions: CDPC security administrator and CDPC administrator;

4.9. Separation of user access rights to CDPC resources in accordance with the security policy;

4.10. Protection against unauthorized interference with CDPC equipment;

4.11. Verification of the integrity and operability of the CDPC Complex of Protection Measures;

4.12. Protection against threats related to the penetration of computer viruses, Trojan programs, use or manifestation of undocumented features or errors in system or application software; countermeasures against access to information obtained in violation of the security policy;

4.13. Monitoring the availability of CDPC equipment and defined resources, with automated real-time alerts;

4.14. Registration and accumulation of audit data, centralized user authentication when accessing CDPC management resources;

4.15. Separation of information resources among different CDPC users.

4.16. Event Logging Requirements:

- Continuous 24/7 logging of user actions—such as authorization, attempted authorization, use of services—and system processes by separate security software tools; logs must be retained for at least 3 months.
- User activity monitoring must ensure the ability to record events defined in the security policy and actions of CDPC users using audit tools and subsequent analysis.

4.17. The Security Measures Suite (KZZ) must log security-related events and provide the security administrator with the ability to view records of these events.

4.18. When a user or process obtains access to CDPC components, the CPM must identify and authenticate the user, determine the entry point, and log the result (successful or unsuccessful) in the system log.

віддаленого доступу до VPC в тестовому режимі або безпосередньо на майданчику Виконавця, попередивши Виконавця про перевірку не менше ніж за 10 робочих днів.

4.6. ХЦОД повинен забезпечувати виконання вимог із захисту персональних даних згідно з Законом України «Про захист персональних даних».

Система захисту інформації ХЦОД повинна забезпечувати:

4.7. відповідальними особами повинні бути розроблені правила розмежування доступу користувачів до ресурсів ХЦОД (порядок надання і розподіл прав адміністраторів та розподіл окремих привілеїв), порядок контролю за їх застосуванням;

4.8. розподіл функцій адміністраторів: адміністратор безпеки ХЦОД, адміністратор ХЦОД;

4.9. розмежування повноважень доступу користувачів до ресурсів ХЦОД згідно з політикою безпеки;

4.10. захист від несанкціонованого втручання в роботу обладнання ХЦОД;

4.11. перевірку цілісності та працездатності КЗЗ ХЦОД;

4.12. захист від загроз, пов'язаних із проникненням комп'ютерних вірусів, «троянських» програм, з використанням або проявом не документованих функцій або помилок системного та прикладного програмного забезпечення; протидію доступу до інформації, який отримується з порушенням політики безпеки;

4.13. перевірку доступності обладнання ХЦОД та визначених ресурсів з оперативним оповіщенням у автоматичному режимі;

4.14. реєстрацію та накопичення даних реєстрації, централізовану автентифікацію користувачів при доступі до ресурсів ХЦОД управління виділеного ресурсу;

4.15. розмежування інформаційних ресурсів для різних користувачів ХЦОД.

4.16. Вимоги до реєстрації подій:

- реєстрація дій користувачів, таких як авторизація, спроба авторизації, використання сервісів тощо та процесів здійснюється безперервно цілодобово окремими програмними засобами захисту та зберігається протягом 3 місяців
- спостереження за діями користувача повинно забезпечити можливість реєстрації подій, які визначені в політиці безпеки та дій користувачів ХЦОД засобами аудиту та їх аналіз.

4.17. Комплекс засобів захисту (КЗЗ) повинен забезпечувати реєстрацію подій, що мають безпосереднє відношення до безпеки та надавати адміністратору безпеки можливість переглядати записи про ці події.

4.18. При отриманні користувачем або процесом доступу до компонентів ХЦОД, КЗЗ повинен ідентифікувати та автентифікувати користувача з визначенням точки входу, і зареєструвати

4.19. Logging tools must make it possible to uniquely identify users or processes associated with security-related events and determine the date and time of each event using appropriate attributes.

4.20. The KZZ must block attempts to carry out threats (attacks), uniquely identify network entities from which such actions originated, and identify users who performed such attempts.

4.21. The security administrator must be able to periodically review the event log to promptly detect actions that may qualify as unauthorized access. The review frequency is determined at the working design stage. It must be possible to automatically send specified types of alerts to the security administrator's console.

5. Requirements for the Physical Environment of the Data Center:

5.1. Backup power system redundancy — at least N+1;

5.2. Cooling system redundancy — at least N+1;

5.3. Physical perimeter security and access control for the Data Center must be ensured;

5.4. A video surveillance system must be in place, with video archives retained for at least 90 days;

5.5. The server room must be equipped with a grounding bus;

5.6. The server room must be equipped with a fire alarm system based on certified equipment, including control panels and smoke detectors;

5.7. The server room must be equipped with an automatic gas fire extinguishing system in accordance with the current design requirements for buildings and premises hosting computing systems;

5.8. The server room must be equipped with a built-in or mobile smoke extraction system;

5.9. Equipment racks must be arranged in rows in compliance with "cold aisle" and "hot aisle" layout requirements;

5.10. Access to the server room must be strictly restricted. Server room doors must have both a mechanical lock and an electronic access control system using contactless cards;

5.11. Power supply to the Data Center must come from two independent sources (first-category connection), and the equipment must be powered by at least two independent power lines;

5.12. Automatic Transfer Switch (ATS) must be present to automatically switch equipment power to an active supply line;

результат (успішний чи неуспішний) в системному журналі.

4.19. Засоби реєстрації повинні надавати можливість однозначно визначити користувачів або процеси, які причетні до подій, що мають безпосереднє відношення до безпеки, а також визначити дату та час події, використовуючи відповідні атрибути.

4.20. КЗЗ повинен забезпечити блокування спроб реалізації загроз (атак), однозначно ідентифікувати мережеві об'єкти, з яких такі дії здійснювались та користувачів, що виконали таку спробу.

4.21. Адміністратор безпеки повинен мати змогу періодично контролювати журнал реєстрації для своєчасного виявлення дій, що можуть кваліфікуватися як несанкціонований доступ. Періодичність контролю визначається на етапі робочого проекту. Має бути реалізована можливість автоматичної передачі попереджень заданих типів на консоль адміністратора безпеки.

5. Вимоги до фізичного середовища ЦОД:

5.1. Резервування системи резервного живлення — не менше N+1;

5.2. Резервування системи охолодження — не менше N+1;

5.3. Забезпечення фізичної охорони периметру ЦОД та контролю доступу;

5.4. Наявність системи відеоспостереження та зберігання відео-архіву не менше 90 днів;

5.5. Серверне приміщення має бути обладнане шиною заземлення;

5.6. Серверне приміщення має бути обладнане системою пожежної сигналізації на базі сертифікованого устаткування. До складу системи повинні входити приймально-контрольні прилади (ППКП) та димові пожежні сповіщувачі;

5.7. Серверне приміщення повинно бути обладнане системою автоматичного газового пожежогасіння, згідно з чинними вимогами з проектування будинків і приміщень для обчислювальних систем;

5.8. Серверне приміщення повинно бути обладнане системою вбудованою або пересувною установкою видалення диму;

5.9. Стійкі з обладнанням повинні бути встановлені в ряди з дотриманням вимог формування «холодних» та «гарячих» коридорів;

5.10. Доступ у серверне приміщення повинний бути строго обмеженим. Двері серверного приміщення повинні бути обладнанні механічним замком та електронним замком с системою доступу на базі безконтактної карти;

5.11. Електроживлення приміщення датацентру від двох незалежних джерел (підключення по першій категорії), обладнанням повинно забезпечуватися електропостачанням від щонайменше двох незалежних ліній живлення;

5.12. АВР (автоматичне введення резерву) для автоматичного перемикання живлення устаткування на працездатний ввід;

5.13. Data Center power must be backed up by uninterruptible power supplies with battery systems and an autonomous power source based on a diesel generator set. Autonomous power redundancy level must be at least N+1;

5.14. Fuel reserves in the Data Center must ensure diesel generator operation at full load for at least 36 hours;

5.15. Temperature, lighting, and humidity levels in the Data Center must comply with sanitary standards, hardware operating requirements, and equipment manufacturer specifications;

5.16. Access to the building where Data Center elements are located must be controlled by security personnel. All Data Center equipment must be located in a dedicated technical zone to minimize access by individuals not involved in equipment maintenance and operation.

5.17. Access to the Data Center premises is permitted only to authorized individuals responsible for maintenance and equipment configuration (administrators). If necessary, third-party individuals may enter only when accompanied by an authorized person with the appropriate permission.

5.18. To prevent unauthorized access to premises containing Data Center equipment, they must be equipped with a security alarm system and video surveillance. Information about door openings must be recorded at the security console, with notifications sent to appropriate qualified personnel authorized to work with the equipment and granted access to the technical zone. The premises must be equipped with ventilation and fire suppression systems.

5.19. The Customer has the right to verify the Data Center's compliance with the requirements specified in this Annex directly at the Contractor's site, provided that the Contractor is notified at least 10 working days in advance.

6. Software Requirements:

6.1. Only licensed software or open-source software that does not require licensing shall be used in the CDPC.

6.2. The Contractor shall provide the Customer with 24/7 technical support regarding the Hypervisor Software, shall maintain partnership relations with the hypervisor software vendor, and shall have certified specialists experienced in working with the virtualization platform / hypervisor software.

6.3. Protection of the CDPC against unauthorized access to information shall be implemented using

5.13. Живлення ЦОД повинно бути резервоване джерелами безперебійного живлення на базі акумуляторних батарей та автономним джерелом живлення на базі дизель-електричної станції. Рівень резервування автономного джерела — не менше N+1;

5.14. Запас палива в ЦОД повинен забезпечувати час автономної роботи дизель-електричної станції під повним навантаженням не менше 36 годин;

5.15. Температура, освітлення та вологість повітря в приміщенні ЦОД має відповідати встановленим вимогам щодо санітарних норм та експлуатації комп'ютерної техніки та вимогам виробників обладнання;

5.16. Вхід до будівлі, де розміщуються елементи ЦОД, контролюється охороною. Все обладнання ЦОД розташовуються в окремому приміщенні технологічної зони з метою мінімізації доступу до приміщення осіб, які не мають відношення до обслуговування та експлуатації обладнання.

5.17. Доступ до приміщення дозволено тільки особам, які мають право доступу для його обслуговування та налаштування обладнання (адміністратори). У разі потреби сторонні особи повинні перебувати в приміщенні тільки у супроводі особи, яка має право доступу до цього приміщення за відповідним дозволом керівництва.

5.18. З метою запобігання несанкціонованому доступу до приміщення, в якому розташовано обладнання ЦОД, їх обладнують системою охоронної сигналізації та засобами відеоспостереження. Інформація щодо відкривання дверей приміщення фіксується на пульті охорони та здійснюється оповіщення відповідних спеціалістів, які мають відповідну кваліфікацію та допущені до роботи з відповідним обладнанням та мають допуск до технологічної території де розміщено ЦОД. Приміщення обладнується системою вентиляції та пожежогасіння.

5.19. Замовник має право на перевірку відповідності ЦОД зазначеним в цьому Додатку вимогам безпосередньо на майданчику Виконавця, попередивши Виконавця про перевірку не менше ніж за 10 робочих днів.

6. Вимоги до програмного забезпечення:

6.1. В ХЦОД повинно використовуватись лише ліцензійне програмне забезпечення, або програмне забезпечення з відкритим кодом, яке не потребує ліцензування.

6.2. Виконавець повинен надавати Замовнику цілодобову технічну підтримку з питань ПЗ Гіпервізора, мати партнерські відносини з виробником ПЗ гіпервізора та сертифікованих фахівців, що мають досвід роботи з платформою віртуалізації\ ПЗ гіпервізора.

6.3. Захист ХЦОД від несанкціонованого доступу до інформації повинен будуватися

software solutions (including specialized network information security systems and network data-transfer tools) that provide appropriate mechanisms (authentication, authorization, and audit) and secure network services.

з використанням ПЗ (у тому числі спеціалізованих систем мережевої інформаційної безпеки та мережевих засобів передачі даних), які мають відповідні механізми (автентифікації, авторизації та аудиту) та захищені мережеві сервіси.

7. Service Availability Requirements

7. Вимоги до доступності Послуг

Table 2. – Service Availability Requirements:

Таблиця 2. – Вимоги до доступності послуг:

No	Parameter Name/ Назва параметру	Value/ Значення
1	Maximum allowable percentage of unplanned Service unavailability/ Максимально допустимий відсоток часу аварійної недоступності Послуги	0.05% (260 minutes per year)/ 0,05 % (260 хвилин на рік)
2	Maximum allowable percentage of unplanned Service quality degradation/ Максимально допустимий відсоток часу аварійного погіршення якості Послуги	0.06% (300 minutes per year)/ 0,06% (300 хвилин на рік)
3	Total percentage of planned Service unavailability (within the maintenance window)/ Сумарний відсоток часу планової недоступності Послуги (у межах вікна обслуговування)	0.11% (600 minutes per year)/ 0,11% (600 хвилин на рік)
4	Total percentage of planned Service quality degradation (within the maintenance window)/ Сумарний відсоток часу планового погіршення якості Послуги (у межах вікна обслуговування)	0.11% (600 minutes per year) 0,11% (600 хвилин на рік)

The total Service unavailability time is calculated proportionally to the duration of Service provision under the Contract./

Сумарний час недоступності послуги розраховується пропорційно терміну надання Послуг по Договору.

8. Requirements for Response and Resolution of Customer Requests

8. Вимоги до реакції та вирішення запитів замовника

Table 3. – Requirements for Response and Resolution of Customer Requests:

Таблиця 3. – Вимоги до реакції та вирішення запитів замовника:

Request Type/ Тип запиту	Schedule/ Регламент	Max Response Time Макс. час реакції	Max Resolution Time (80% of requests)/ Макс. час виконання (80% запитів)	Maximum Resolution Time (99% of requests)/ Макс. час виконання (99% запитів)
Incident/ Інцидент	24/7	30 minutes/ 30 хвилин	3 hours/ 3 години	12 hours/ 12 годин
Change/ Зміна	Business hours/ Бізнес-час	2 business-hours/ 2 бізнес-години	8 business-hours/ 8 бізнес-годин	55 business-hours/ 55 бізнес-годин
Consultation/ Консультація	Business hours/ Бізнес-час	2 business-hours/ 2 бізнес-години	12 business-hours/ 12 бізнес-годин	60 business-hours/ 60 бізнес-годин