CONTRACT OF ICT INFRASTRUCTURE

KNOW ALL MEN BY THESE PRESENTS:

This contract is entered is entered into this__ day of **FEB 0 7 2023**, by and between :

DEPARTMENT OF EDUCATION REGIONAL OFFICE IV-A CALABARZON, a component field office of the government entity known as the Department of Education organized under existing Philippine laws with office address at Gate 2, Karangalan Village, Cainta, Rizal and herein represented by its Regional Director, **ATTY. ALBERTO T. ESCOBARTE.** It shall be referred in this agreement as the **DepEd.**

-and-

HYPERNET – INTERNET & BUSINESS SOLUTIONS INC. is corporation duly organized under and by law. It is represented in this contract by its Sales Account Executive, **SUNSHINE C. FRANCISCO,** with office address at 1266 Unit G Marianne Townhomes G. Del Pilar cor. P. Ocampo St., Malate, Manila hereinafter referred to as the **SUPPLIER.**

WHEREAS, Procuring Entity has undertaken the procurement of **"ICT INFRASTRUCTURE"**.

WHEREAS, Section 53.9 of the 2016 Revised Implementing Rules and Regulations (R-IRR) of Republic Act 9184, otherwise known as the "Government Procurement Reform Act of 2003", allows an agency to resort to Small Value Procurement as alternative methods of procurement where the amount involved does not exceed the threshold amount of One Million Pesos (Php1,000,000.00) as prescribed in Annex "H" thereof;

WHEREAS, the Approved Budget for the Contract (ABC) is **NINE HUNDRED SIXTY THOUSAND PESOS ONLY (Php960,000.00);**

WHEREAS, the Request for Quotation (RFQ) was posted in the Philippine Government Electronic Procurement System (PhilGEPS) website on December 20, 2022, in office website, and in conspicuous bulletin board in the premises of this Office on December 19, 2022 to December 26, 2022;

WHEREAS, RFQs were sent to at least four (4) prospective suppliers namely:

1. IP Solution Inc.;
2. Hypernet – Internet & Business Solutions Inc.;
3. NetFrasys; and
4. Cloudbytes

Address: Gate 2, Karangalan Village, Cainta, Rizal
Telephone Nos.: 02-8682-5773/8684-4914/8647-7487
Email Address: region4a@deped.gov.ph
Website: depedcalabarzon.ph

WHEREAS, one (1) Supplier submitted its proposal: **HYPERNET – INTERNET & BUSINESS SOLUTIONS INC.** in the amount of **NINE HUNDRED FIFTY-EIGHT THOUSAND NINE HUNDRED FIFTY PESOS ONLY (Php958,950.00).** Thus the **Supplier** was declared as the lone bidder.

WHEREAS, after review and deliberation on the proposal, the **Supplier** complied with the requirements and declared as the Single Calculated and Responsive Bid (SCRB);

WHEREAS, pursuant to the Implementing Rules and Regulations of Republic Act 9184, the Bids and Awards Committee of DepEd CALABARZON recommended on December 29, 2022 to the head of the procuring entity the award of the project to **Supplier.**

NOW, THEREFORE, for and in consideration of the premises, the parties hereby agreed as follows:

Section 1
Responsibiliy of the Supplier

The Supplier shall deliver the following items/products:

Item	Description	QTY	Total Cost (VAT Inclusive)
1.	Data Firewall (Php395,000.00)	1 set	Php395,000.00
2.	M.2 SSD (Php7,000.00)	15 pcs	105,000.00
3.	High End – Laptop (Php100,000.00)	2 pcs	200,000.00
4.	Handy Vacuum with Blower (Computer) (Php3,000.00	1 pc	3,000.00
5.	UPS for Server (Php50,000.00)	2 pcs	100,000.00
6.	Network Tester	1 pc	49,000.00
7.	Pass through RJ45 (Php600.00)	5 bots	3,000.00
8.	Computer Tool Kit (Php4,000.00)	2 pcs	8,000.00
9.	Touch Screen (Php28,000.00)	1 pc	28,000.00
10.	CAT 6 UTP Cable (Php9,000.00)	1 box	9,000.00
11.	Internet Loader/Balancer (Php33,000.00)	1	32,950.00
12.	Installation, configuration and set-up of component, testing, conditioning and training (Php26,000.00)	1 Lot	26,000.00

with the following Technical Specifications:

1. NEXT GENERATION DATA FIREWALL

Next Generation Data Firewall Technical Compliance Table

TECHNICAL SPECIFICATIONS:

Performance	The proposed solution must have 4 Gbps Firewall Layer 3 throughout
	The proposed solution must support at least 1,200,000 concurrent sessions
	The proposed solution must support at least 30,000 new connections per second
Interface	The proposed solution must have at least 6*10/100/1000 Base-T
Management	Management console must be managed through Web interfaces via secure encrypted connection
	The proposed solution must support policy configuration modules for the following functions from a single appliance - Stateful firewall - DDos Prevention, ARP spoofing prevention - Anti-Virus - Anti-Malware, On-premise artificial intelligence based malware detection engine - Anti-phising - Instruction Prevention System - SSL Decryption - Risk assessment by on-demand and real-time scanner - Cloud sanboxing - Cloud threat intelligence - IPsec VPN - SSL VPN - User authentication and grouping - Web(URL) filtering, Application control, Bandwidth management - Report center
	The proposed solution must support security protection for pre-attack, during-attack and post-attack
	The proposed solution must support security protection for business systems and network users
FW	The proposed solution must support static and dynamic package filtering, Inspection on well-known protocols of FTP, HTTP, SMTP, RTSP, H.323 (Q.931, H.245, RTP/RTCP), SQLNET, NMS, PPTP, TCP, UDP...
	The proposed solution must be able to protect against attacks of Land, Smurf, Fraggle, WinNuke, Ping of Death, Tear Drop, IP spoofing, SYN/ICMP/UDP flood, HTTP GET flood, DNS query flood, ARP cheating, ICMP redirection, static and dynamic blacklist, etc.
	Country block, create rules to allow or block traffic from IP addresses in specific countries, regions and states, reduce the attack possible
	Supports real-time integration status between the local firewall and the cloud threat intelligence but not limited by providing: - The total number of external attack events - The number of threats detected by Cloud Treat Intelligent in the local firewall

Instruction Prevention System	The proposed solution must support vulnerability database with at least 4000+ entries
	The proposed solution must support separate server and endpoint vulnerability database group for convenient policy configuration
	The IPS system must be able to block worms, Trojans, spyware, scanning, DoS, DDoS, vulnerability exploits, buffer overflow attacks, abnormal protocol and attacks with evasive tactic employed.
	The IPS supports automatically block, logging, upload gray threat to the "cloud"
	The IPS supports burp-force attack prevention for FTP, IMAP MSSQL, POP3 SMTP, ORACLE, RDP, SMBv1, SMBv2, SMBv3 and so on.
APT Prevention	The proposed solution must support APT detection of identifying botnet, remote control trojans, malicious link, and other threats.
	The proposed solution must support anti-malware database with more than 400,000+ entries
	The proposed solution must be able to conduct cross-module intelligent correction of IPS and APT detection module, that to generate temporary FW rules to lock the suspicious IP when malicious behavior from that IP is detected by any of the modules.
	APT supports sandbox dynamic detection via security cloud
	APT supports to detect DDos attack from intranet
	APT can effectively distinguish the hazardous traffic flow in the common application of the RDP, SSL, IMAP, SMTP, POP3, FTP,, DNS,, HTTP, WEB, and so on traffic flow , but also can be used for the normal operation of non standard port for early warning
	Support honeypot feature and locate the real host IP address of the intranet infected botnet virus
	Support in-depth analysis on detected malware or trojan behaviors by demonstrating interaction & communication between external C&C botnets and others suspicious events
Risk Assessment and Prevention	The proposed solution must provide risk assessment module that allows to scan and identify security loopholes such as open port, system vulnerabilities, weak passwords and other risks of the protected servers
	The proposed solution must support built-in Web Scanner (None 3rd Party tools) that allows to scan targeted website/URL to discover the system vulnerabilities of including but not limited to SQL injection, xss, csrf, Dictionary Traversal, Commend execution, etc.
	Risk assessment and scanning results must be shown and generated with corresponding reports with detailed description of the issues and recommended solution.
	Risk assessment module must be able to be affiliated with the IPS to automatically generate the protection policies
	Threat Alerts is able to actively push the current popular 0 day or high-risk vulnerabilities, and can provide vulnerability detection tools for business scan, according to the results of scan, it can generate safety protection policies
Anti-Virus	Stream-based anti-virus for HTTP, FTP, SMTP and POP3 , protocols, etc.

	The proposed solution must support built-in Artificial Intelligence capability to detect malware, virus and ransomware variants and provide the malware analysis report
	Should support compressed file malware inspection
	Should support cloud based threat intelligence and analytics
Content Security	Mail protect support pop3, smtp, imap, pop3s, smtps, imaps and other specific port.
	Mail protect support mail collision attack prevention and anti-phishing.
	Mail attachment can be detected by anti-virus.
	Support mail attachment filter and http/ftp download/upload filter.
	When users receive Malicious Mail, The proposed solution will tamper the mail subject
Access Management	The proposed solution must support up to eight user identification methods such as active directory (AD) authentication and Remote Authentication Dial-In User Service (RADIUS)
	The proposed solution should support Internet application identification database with more than 2800+ entries and URL database with more than hundreds of millions entries that updated with cloud-based technologies
	The proposed solution must support policy configuration oriented toward users and applications for web filter, application control and bandwidth management
	The proposed solution must support link load balance per traffic load as well as application type in occasion of multiple Internet lines
Reporting	The proposed solution must support built-in report center, which provides comprehensive security analyzing reports including but not limit to attack trends by "All attacks" and "Valid Attacks"; "user security" and "vulnerability" ; Vulnerability assessment
	Support the detailed loges for security issues as DOS attack, IPS, viruses, website access, application control, user login and OS configuration
	The report center must provide full visibility to network, endpoint clients with multi-dimensional analysis of risks, vulnerabilities, attacks, threats, traffic and behaviors
	Support PDF format and automatically send to pre-defined mailbox on daily/weekly/monthly basis
	"Supports automatic generation of comprehensive security risk reports. The content of the report should reflect but not limited: - The overall security level of the protected network object - The vulnerability information & forensic evidence each attack"
Deployment	"The proposed solution must support following deployment options - Gateway (Route mode) - Bridge mode - Mirror mode - Multiple Bridge mode (2- 4 bridges)"
	The proposed solution must support build-in auto hardware bypass in the event of hardware failure

	Support quick deployment from central management console
VPN	The proposed solution must support Private VPN
	"IPSEC VPN
	Authentication algorithm: MD5/SHA-1 Encryption algorithm: DES/3DES/AES128 Hash:MD5/SHA"
	"SSL VPN : source type: L3VPN resources, TCP resources. source type: L3VPN resources, TCP resources. os: win xp/win 7/win 8/win 10/mac"
Real-time visibility	Real time provides CPU, memory, disk usage, session number, the number of online users, the network interface, box resource information
	The proposed solution must be provide real-time user ranking / real-time application ranking / real-time host ranking
	The proposed solution must be provide real-time attack map, include top atack country and counting, real-time attack and threat detail
	Provide information security incidents, including recently security incidents, server security incidents, terminal security incidents
	In security status, it display the current network risks need to be handled, and top attascks, bots show the threat stage and security rating
	Top session can display Real-time, Last 24 hours, Last 7 days of the current session and the new session
Routing	Supports static route, ECMP, RIPv1 & v2, OSPFv2 and BGP
	The proposed solution must be able to support but not limited to intellegient route selection based on source and destination IP, Port, Protocol and country based IP address
	Support DNS-Mapping
	Support custom intranet DNS server address to avoid botnet detection misjudgment DNS server
Certification	"The proposed solution must be a member of MAPP(The Microsoft Active Protections Program)
	The proposed solution must be certificated by ICSA Labs
	The proposed solution must have AAA Rating at CyberRatings Enterprise Firewall
	The IPS vulnerability database must be CVE Compatibility certificated
	In order to ensure the maturity of solution technology, the principal must be CMMI L5 certified"
Additional	Complimentary 30 Units of Endpoint Security Agent Licenses for 1YR.
	Complimentary Endpoint Security Management
	Complimentary Incident Response (Once per annum)
Vendor Qualifications	Must have a Certified Engineer of the brand offer
	Must have a Certificate of Partnership of the Brand Offer
Knowledge transfer	The supplier kmow how to conduct transfer knowledge to the end user(ICT Unit Personnel)
	The supplier must install and configure the appliance to the on premise data center

2. **1TB HDD or higher (2.5") M.2 NVMe SSD**

3. **Windows 11 Home or Higher (64-bit)**
   2th Gen Intel® Core™ i7-12650H Processor 2.3 GHz or Higher
   (24M Cache, up to 4.7 GHz, 10 cores: 6 P-cores and 4 E-cores)
   or higher
   NVIDIA® GeForce RTX™ 3050Ti
   15.6"" WQHD (2560x1440) IPS Level
   16GB DDR5-4800 SO-DIMM or higher
   512GB M.2 NVMe™ PCIe® 3.0 SSD
   preferable branded
   must be in 3 years warranty and support period"

4. • ▶**Wattage: 800W or higher**
   • ▶**Frequency: 60Hz or higher**
   • ▶**Voltage: 220V**
   • ▶**Thermal Protection 105°C**
   • ▶**Material: ABS Plastic**
   • ▶**Dust capacity: 0.5L**
   • ▶**Air Flow: 840 1/minFEATURES:**
   • ▶**Suitable for vacuuming various types of dirt (Ex. Wood, Plastic or Metal Chips)**
   • ▶**Ideal for Hard to Reach areas thanks to the crevice nozzle**
   • ▶**Comfortable to use thanks to compact , low weight, and ergonimic designINCLUSIONS:**
   • ▶**1pc Round Cleaning Brush**
   • ▶**1pc 2 in 1 Brush/Crevice tool**
   • ▶**1pc Plastic Hose**
   • ▶**1pc Belt**
   • ▶**1pc Filter with Dust Cup (can be used as blower) Preferable branded**
     1 year warranty and support period"

5. **"High frequency, On-line Smart UPS, Rack-Tower Convertible, Hot-Swappable Battery Module Design, Standard Unit, 3KVA/2.7 KW, PF: 0.9, 72Vdc, with 6pcs X 9Ah built-in battery, with USB, RS232, EPO , SNMP function Port, with Colorful LCD**

   Vendor Qualifications:
   • Must be a Certified Partner/Reseller of the Brand
   • Preferable branded.
   • 1 year warranty and support period

6. **IntelliTone digital toning eliminates noise and false signals SmartTone analog toning precisely isolates individual wire Pairs**

   Locates cables safely and effectively on active networks Verifies twisted pair installation with visual end to end continuity test Probe detects digital signal and 1 kilo hertz signal from the analog toner Probe has built in pair tester to identify open, shorted and crossed pairs Signal strength indicator LEDs so you can help identify 1 cable that is bundled with other cablesConfirms cable location, verifies cable continuity, and detects cable faults (opens, shorts, and reversed pairs) in 1 step atleast branded
   1 years warranty and support period"

7. RJ45 CAT6 Passthrough FTP Network Modular Plug Connector Pass Through Unshielded
- 1 year warranty and support period

8. Passtrough Network Tool Set
- preferable branded
- 1 year warranty and support period

9. 23.8" IPS Touch Monitor | Capacitive 10 Point Touch, FHD 1920 x 1080 @ 60Hz, Smart Image, Low Blue Light, IP54 Touch Surface, 5-90 degrees Tilt / 10-70 degrees Fold, VESA
- preferable branded
- 1 year warranty and support period

10. Cat 6 UTP Cable
- preferable branded

11. Internet Loader/Balancer
- preferable branded
- 1 year warranty and support period

12. Installation, Configuration, testing, commissioning, training and Setup of Components

Vendor Qualification:
- Atleast must have a Certified Engineer of the brand offer
- Atleast must have a Certificate of Partnership of the Brand offer

within thirty (30) days (contract time) from the execution of this contract.

More, in consideration of the payment, the Supplier hereby covenants to provide the goods and services and to remedy defects therein in conformity in all respects with the provisions of the contract including the warranty provisions for each item.

Section 2
Place and Manner of Delivery and Inspection

The **Supplier** shall deliver the items to the Asset Section of the Regional Office. It shall be inspected by the ICT Unit of DepEd before acknowledging receipt of the deliveries.

In case there was failure of the **Supplier** to make delivery within the contract time, **DepEd** shall require the **Supplier** to explain in writing the reason of the delay. This is without prejudice to the right of DepEd to impose liquidating damages and other administrative penalties.

The items/products must conform to and comply with the technical specifications provided in Section 1. Any proposal by the Supplier to deliver goods of different technical specification in lieu of the technical specifications provided in Section 1, shall be rejected by DepEd.

section 3
Responsibility of DepEd

The **DepEd** shall pay the **Supplier** the amount of **NINE HUNDRED FIFTY-EIGHT THOUSAND NINE HUNDRED FIFTY PESOS ONLY (Php958,950.00).** In case there is partial delivery as indicated in the Inspection and Acceptance Report, DepEd shall pay in proportion to the items delivered.

Section 4
Assignment

The **Supplier** shall neither assign, transfer, pledge, nor sub-contract any part or interest therein.

Section 5
Terms of Contract

Any party may terminate this Contract based on the grounds provided and after compliance with Annex "I" of the 2016 Implementing Rules and Regulations of Republic Act 9184.

Section 6
Liquidating Damages

Liquidated damages equivalent to one tenth of one percent (0.1%) of the value of the goods not delivered within the prescribed delivery period shall be imposed per day of delay. DepEd shall rescind the contract once the cumulative amount of liquidated damages reaches ten percent (10%) of the amount of the contract, without prejudice to other course of action and remedies open to it.

Section 7
Dispute

The parties shall make every effort to resolve amicably and by mutual consultation any or all disputes or differences arising between the Parties in connection with the implementation of this contract. Should such dispute not be resolved amicably, it shall be submitted to arbitration in the Philippines according to the provisions of Presidential Decree No. 242 and Executive Order No. 292. Provided, however, that by mutual agreement, the parties may agree in writing to resort to other alternative modes of dispute resolution.
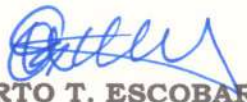
Section 8
Attestation

The Supplier attest that its signatory is duly authorized by its Board and/or its management to sign for and in its behalf.

IN WITNESS WHEREOF, the parties have hereunto set their hands, this day of
FEB 0 7 2023 at   CITY OF MANILA   , Philippines.

Department of Education
Region IV-A CALABARZON

ATTY. ALBERTO T. ESCOBARTE, CESO II
Regional Director

Hypernet-Internet &
Business Solutions Inc.

SUNSHINE C. FRANCISCO
Sales Account Executive

SIGNED IN THE PRESENCE OF:

REY M. VALENZUELA
ITO, ICT Unit

Republic of the Philippines
_____CITY OF MANILA_____ S.S.

ACKNOWLEDGMENT

BEFORE ME, a Notary Public for and in the City of CITY OF MANILA , this
FEB 0 7 2023 , personally appeared:

Name	Identification No.	Expiration Date
Atty. Alberto T. Escobarte	DepEd Office ID No. 4529876	_____
Sunshine C. Francisco	UMID ID. 0113-0683113-4	_____

who are known to me and to me known to be the same persons who executed the foregoing instrument and acknowledged to me that the same is their own free act and voluntary act and deed.

This instrument, consisting of ten (10) pages, including the page on which this acknowledgment is written, has been signed on the left margin of each and every page hereof by the concerned parties and their witnesses, and sealed with my notarial seal.

WITNESS MY HAND AND SEAL, at the place and date above-written.

Notary Public

Doc. No. 731..;
Page No. 147..;
Book No. 1.....;
Series of 2023.

ATTY. GILBERTO B. PASIMANERO
Notary Public until December 31, 2023
Notarial Commission 2022 - 052
IBP# 165727; Pasig for yr. 2023
PTR# 0861164; Mla - 1-3-2023
Roll # 25473; TIN# 103-098-346
MCLE Exempt No. VII-NP004370 'til 4-14-2025