GOVERNMENT PROCUREMENT CONTRACT

Procurement of IT Infrastructure and Managed Services

Department of Information and Communications Technology

Effective: January 15, 2025

Expiration: January 14, 2028

Contract Value: PHP 48,500,000.00

GOVERNMENT PROCUREMENT CONTRACT

CONTRACT NO. GPC-2025-0847

REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF INFORMATION AND

COMMUNICATIONS TECHNOLOGY (DICT)

PROCUREMENT OF IT INFRASTRUCTURE

AND MANAGED SERVICES AGREEMENT

Effective Date: January 15, 2025

Expiration Date: January 14, 2028

Contract Value: PHP 48,500,000.00

TABLE OF CONTENTS

ARTICLE XIII — DISPUTE RESOLUTION

ARTICLE XIV — GENERAL PROVISIONS

ANNEXES A-F

ARTICLE I — PARTIES AND RECITALS

This Procurement Contract ("Contract") is entered into by and between:

THE GOVERNMENT OF THE REPUBLIC OF THE PHILIPPINES, represented by the DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY (DICT), with principal office at C.P. Garcia Avenue, Diliman, Quezon City 1101, represented herein by its Secretary, HON. MARIA ELENA C. SANTOS, hereinafter referred to as the "PROCURING ENTITY";

— and —

PACIFIC DIGITAL SOLUTIONS, INC., a corporation duly organized and existing under the laws of the Republic of the Philippines, with principal office at 15th Floor, Pacific Star Building, Makati Avenue corner Gil Puyat Avenue, Makati City 1226, represented herein by its President and CEO, MR. ROBERTO A. VILLAROSA, hereinafter referred to as the "SUPPLIER";

WHEREAS, the Procuring Entity conducted a public bidding for the Procurement of IT Infrastructure and Managed Services (Bid Reference No. DICT-2024-ICT-0392) in accordance with Republic Act No. 9184, otherwise known as the "Government Procurement Reform Act," and its Revised Implementing Rules and Regulations;

WHEREAS, the Supplier submitted the Lowest Calculated and Responsive Bid in the amount of FORTY-EIGHT MILLION FIVE HUNDRED THOUSAND PESOS (PHP 48,500,000.00), inclusive of all applicable taxes;

WHEREAS, the Bids and Awards Committee (BAC) has recommended the award of the contract to the Supplier, and the Head of the Procuring Entity

has approved said recommendation;

NOW, THEREFORE, for and in consideration of the foregoing premises and the mutual covenants herein contained, the parties agree as follows:

ARTICLE II — SCOPE OF WORK

Section 2.1 — General Description

The Supplier shall provide the following goods and services to the Procuring Entity:

(a) Supply, delivery, installation, and configuration of IT infrastructure equipment as specified in Annex A (Technical Specifications);

(b) Provision of managed IT services including network monitoring, helpdesk support, and system administration for the contract duration as specified in Annex B (Service Requirements);

(c) Training and capacity building for DICT personnel as specified in Annex C (Training Plan);

(d) Data migration services from legacy systems as specified in Annex D (Migration Plan).

Section 2.2 — Detailed Requirements

2.2.1 Hardware Infrastructure:
- Forty (40) units enterprise-grade rack servers with minimum specifications: Intel Xeon Gold 6448Y processor, 512GB DDR5 RAM, 4x 1.92TB NVMe SSD in RAID-10 configuration
- Ten (10) units network switches, 48-port 25GbE with 8x 100GbE uplinks, managed, stackable
- Five (5) units enterprise firewall appliances with IPS/IDS, minimum 40Gbps throughput

- Two (2) units enterprise storage arrays, minimum 500TB usable capacity, NVMe-oF capable
- Twenty (20) units uninterruptible power supply, 10kVA online double-conversion

2.2.2 Software Licenses:

- Enterprise virtualization platform for 40 hosts (3-year license)
- Network monitoring and management suite (3-year subscription)
- Backup and disaster recovery solution (3-year license)
- Endpoint protection for 500 seats (3-year subscription)

2.2.3 Managed Services:

- 24/7 Network Operations Center (NOC) monitoring
- Helpdesk support (Tier 1 through Tier 3)
- Quarterly infrastructure health assessments
- Monthly security vulnerability scanning and remediation
- Annual disaster recovery testing and documentation

Section 2.3 — Project Sites

All equipment shall be delivered, installed, and commissioned at the following locations:

Primary Site: DICT Main Data Center, Quezon City
Secondary Site: DICT Disaster Recovery Site, Clark, Pampanga
Regional Offices: Cebu, Davao, Baguio (network equipment only)

ARTICLE III — CONTRACT PRICE AND PAYMENT TERMS

Section 3.1 — Contract Price

The total contract price is FORTY-EIGHT MILLION FIVE HUNDRED THOUSAND PESOS (PHP 48,500,000.00), broken down as follows:

(a) Hardware and Equipment: PHP 32,150,000.00

(b) Software Licenses (3-year): PHP 6,800,000.00

(c) Managed Services (3-year): PHP 7,200,000.00

(d) Training and Capacity Building: PHP 1,350,000.00

(e) Data Migration Services: PHP 1,000,000.00

_____

TOTAL: PHP 48,500,000.00

Section 3.2 — Payment Schedule

Payment shall be made according to the following milestone-based schedule:

Milestone 1 — Upon delivery and acceptance of all hardware equipment at the Primary Site:
Payment: PHP 16,075,000.00 (50% of hardware cost)

Milestone 2 — Upon successful installation, configuration, and commissioning of all equipment at all sites:
Payment: PHP 16,075,000.00 (remaining 50% of hardware cost)

Milestone 3 — Upon completion of data migration and user acceptance testing:
Payment: PHP 1,000,000.00 (data migration)
Payment: PHP 1,350,000.00 (training)

Milestone 4-15 — Quarterly managed services payments:
Payment: PHP 600,000.00 per quarter (PHP 7,200,000 / 12 quarters)

Milestone 16 — Final payment upon completion of 3-year software license period:
Payment: PHP 6,800,000.00 (software licenses — paid upon delivery of license certificates and activation confirmation)

Section 3.3 — Invoicing Requirements

The Supplier shall submit the following with each invoice:

(a) Original invoice in triplicate

(b) Delivery receipt signed by authorized DICT representative

(c) Acceptance certificate for the applicable milestone

(d) Progress report for managed services (quarterly payments)

(e) Updated asset inventory report

Section 3.4 — Payment Processing

Payment shall be processed within thirty (30) calendar days from receipt of complete billing documents. Late payment by the Procuring Entity shall not entitle the Supplier to suspend services.

Section 3.5 — Taxes

The contract price is inclusive of all applicable taxes, duties, and fees. The Supplier shall be responsible for the payment of all taxes arising from this Contract.

ARTICLE IV — DELIVERY AND IMPLEMENTATION SCHEDULE

Section 4.1 — Overall Timeline

The project shall be implemented according to the following schedule:

Phase 1 — Hardware Delivery (Days 1-45):

- All hardware equipment delivered to Primary Site within 30 calendar days from Notice to Proceed
- Equipment for Secondary Site and Regional Offices delivered within 45 calendar days from Notice to Proceed

Phase 2 — Installation and Configuration (Days 31-90):

- Primary Site installation: Days 31-60
- Secondary Site installation: Days 46-75
- Regional Offices installation: Days 46-90
- Network interconnection and testing: Days 75-90

Phase 3 — Data Migration (Days 76-120):

- Legacy system assessment: Days 76-85
- Data extraction and transformation: Days 86-100
- Data loading and validation: Days 101-110
- User acceptance testing: Days 111-120

Phase 4 — Training (Days 91-135):

- System administrator training: Days 91-105
- End-user training: Days 106-120
- Knowledge transfer documentation: Days 121-135

Phase 5 — Managed Services (Days 121-1095):

- Service commencement: Day 121
- Quarterly health assessments
- Annual DR testing
- Contract completion: Day 1,095 (3 years from NTP)

Section 4.2 — Notice to Proceed

The Procuring Entity shall issue the Notice to Proceed (NTP) within seven (7) calendar days from the date of contract signing. The Supplier shall commence work within seven (7) calendar days from receipt of the NTP.

Section 4.3 — Delivery Inspection

All deliveries shall be inspected by the DICT Inspection Committee within five (5) working days from delivery. Equipment failing inspection shall be replaced within fifteen (15) calendar days at the Supplier's expense.

ARTICLE V — SERVICE LEVEL AGREEMENTS (SLA)

Section 5.1 — Availability Requirements

The Supplier shall maintain the following availability levels for all managed services:

Critical Systems (servers, storage, firewalls):
- Required Availability: 99.95% per month
- Maximum Allowable Downtime: 21.9 minutes per month
- Measurement: Automated monitoring with monthly reports

Network Infrastructure (switches, connectivity):
- Required Availability: 99.90% per month
- Maximum Allowable Downtime: 43.8 minutes per month
- Measurement: Automated monitoring with monthly reports

Helpdesk Services:
- Required Availability: 99.5% during business hours (8AM-5PM)
- 24/7 availability for Critical and High severity incidents

Section 5.2 — Incident Response Times

The Supplier shall respond to and resolve incidents within the following timeframes:

Critical (System Down):
- Response Time: 15 minutes
- Resolution Time: 4 hours
- Escalation: Immediate notification to DICT IT Director

High (Degraded Performance):
- Response Time: 30 minutes
- Resolution Time: 8 hours
- Escalation: Notification to DICT IT Director within 1 hour

Medium (Non-Critical Issue):
- Response Time: 2 hours
- Resolution Time: 24 hours
- Escalation: Weekly summary report

Low (Service Request):

- Response Time: 4 hours

- Resolution Time: 72 hours

- Escalation: Monthly summary report

Section 5.3 — SLA Reporting

The Supplier shall provide the following reports:

(a) Monthly SLA performance report — due within 5 working days after end of month

(b) Quarterly infrastructure health assessment — comprehensive report with recommendations

(c) Annual security posture assessment — including vulnerability scan results and remediation status

(d) Incident post-mortem reports for all Critical incidents — within 48 hours of resolution

Section 5.4 — SLA Credits

Failure to meet SLA targets shall result in service credits as follows:

Availability below target by 0.01% - 0.05%:

Credit: 5% of monthly managed services fee

Availability below target by 0.06% - 0.10%:

Credit: 10% of monthly managed services fee

Availability below target by more than 0.10%:

Credit: 20% of monthly managed services fee

Repeated SLA failures (3 consecutive months):

Credit: 25% of monthly managed services fee plus mandatory remediation plan within 10 working days

ARTICLE VI — PENALTY CLAUSES AND LIQUIDATED DAMAGES

Section 6.1 — Delay in Delivery

For every calendar day of delay in the delivery of hardware equipment beyond the contractual delivery date, the Supplier shall pay liquidated damages equivalent to ONE-TENTH OF ONE PERCENT (0.1%) of the cost of the undelivered items for each day of delay.

Maximum cumulative penalty for delivery delays: TEN PERCENT (10%) of the total hardware cost (PHP 3,215,000.00).

If the delay exceeds ONE HUNDRED (100) calendar days, the Procuring Entity may terminate the contract and forfeit the performance security.

Section 6.2 — Delay in Installation

For every calendar day of delay in the completion of installation and commissioning beyond the contractual completion date, the Supplier shall pay liquidated damages equivalent to ONE-TENTH OF ONE PERCENT (0.1%) of the total contract price for each day of delay.

Maximum cumulative penalty for installation delays: TEN PERCENT (10%) of the total contract price (PHP 4,850,000.00).

Section 6.3 — SLA Penalty for Managed Services

In addition to SLA credits specified in Section 5.4, persistent failure to meet SLA targets shall incur the following penalties:

(a) Three (3) consecutive months of SLA failure: Penalty: PHP 100,000.00 per occurrence

(b) Six (6) months of SLA failure within any 12-month period: Penalty: PHP 250,000.00 plus mandatory service improvement plan at Supplier's cost

(c) Nine (9) or more months of SLA failure within any 12-month

period:

Grounds for contract termination for default, with forfeiture of performance security

Section 6.4 — Data Breach Penalty

In the event of a data breach attributable to the Supplier's negligence or failure to implement required security measures:

(a) First occurrence:

Penalty: PHP 500,000.00 plus full cost of breach notification and remediation

(b) Second occurrence:

Penalty: PHP 1,000,000.00 plus grounds for contract termination for default

(c) The Supplier shall notify the Procuring Entity of any suspected data breach within FOUR (4) HOURS of discovery.

(d) The Supplier shall bear all costs associated with breach investigation, notification to affected parties, and compliance with National Privacy Commission requirements under Republic Act No. 10173.

Section 6.5 — Penalty for Non-Compliance with Reporting

Failure to submit required reports within the specified timelines:

Monthly SLA reports:

Penalty: PHP 10,000.00 per report per day of delay

Quarterly health assessments:

Penalty: PHP 25,000.00 per report per day of delay

Incident post-mortem reports:

Penalty: PHP 15,000.00 per report per day of delay

Section 6.6 — Penalty Cap

The total accumulated penalties under this Article shall not exceed TWENTY PERCENT (20%) of the total contract price (PHP 9,700,000.00). Upon reaching the penalty cap, the Procuring Entity reserves the right to terminate the contract for default.

ARTICLE VII — WARRANTY AND MAINTENANCE

Section 7.1 — Hardware Warranty

The Supplier warrants all hardware equipment against defects in materials and workmanship for a minimum period of THREE (3) YEARS from the date of acceptance, with the following coverage:

(a) On-site, next-business-day replacement for all server and storage components

(b) 4-hour response for critical infrastructure components (firewalls, core switches)

(c) Advance replacement for non-critical components

Section 7.2 — Software Warranty

All software shall be warranted for the full license period with:

(a) Access to all updates and patches

(b) Vendor technical support

(c) Bug fixes and security patches within 24 hours of vendor release

Section 7.3 — Extended Warranty Option

The Procuring Entity reserves the right to extend hardware warranty coverage for an additional TWO (2) YEARS at a pre-agreed price not exceeding FIFTEEN PERCENT (15%) of the original hardware cost per

year of extension.

ARTICLE VIII — INTELLECTUAL PROPERTY RIGHTS

Section 8.1 — Ownership

All custom software, configurations, scripts, documentation, and other deliverables created specifically for the Procuring Entity under this Contract shall be the exclusive property of the Government of the Republic of the Philippines.

Section 8.2 — License Grant

The Supplier grants the Procuring Entity a perpetual, irrevocable, non-exclusive license to use all third-party software components included in the deliverables, subject to the terms of the respective software licenses.

Section 8.3 — Source Code Escrow

For all custom-developed software, the Supplier shall deposit the source code, build instructions, and documentation with a mutually agreed escrow agent within thirty (30) days of acceptance. The escrow shall be released to the Procuring Entity upon:

(a) Supplier's insolvency or dissolution

(b) Material breach by the Supplier

(c) Supplier's failure to provide required maintenance

ARTICLE IX — CONFIDENTIALITY AND DATA PRIVACY

Section 9.1 — Confidentiality Obligations

The Supplier, its employees, agents, and subcontractors shall

maintain strict confidentiality of all information, data, and documents obtained in connection with this Contract. This obligation shall survive the termination or expiration of this Contract for a period of FIVE (5) YEARS.

Section 9.2 — Data Privacy Compliance

The Supplier shall comply with Republic Act No. 10173 (Data Privacy Act of 2012) and its Implementing Rules and Regulations, including but not limited to:

(a) Appointment of a Data Protection Officer

(b) Implementation of reasonable and appropriate organizational, physical, and technical security measures

(c) Ensuring that personal data is processed only for the purposes specified in this Contract

(d) Notification to the Procuring Entity and the National Privacy Commission of any personal data breach within seventy-two (72) hours of discovery

(e) Execution of a Data Sharing Agreement as required by NPC Circular No. 2016-02

Section 9.3 — Data Handling Requirements

(a) All data shall be stored within the territory of the Philippines unless explicitly authorized in writing by the Procuring Entity

(b) Data encryption at rest (AES-256 minimum) and in transit (TLS 1.2 minimum)

(c) Access controls based on principle of least privilege

(d) Audit trails for all data access and modifications

(e) Secure data disposal upon contract termination using NIST 800-88 guidelines

Section 9.4 — Personnel Security

All Supplier personnel assigned to this project shall:

(a) Undergo background checks at the Supplier's expense

(b) Sign individual non-disclosure agreements

(c) Complete data privacy awareness training

(d) Be subject to DICT security policies while on-site

ARTICLE X — INSURANCE AND INDEMNIFICATION

Section 10.1 — Insurance Requirements

The Supplier shall maintain the following insurance coverage for the duration of the Contract:

(a) Comprehensive general liability: PHP 10,000,000.00

(b) Professional liability / errors and omissions: PHP 5,000,000.00

(c) Cyber liability insurance: PHP 10,000,000.00

(d) Workers' compensation as required by Philippine law

Section 10.2 — Indemnification

The Supplier shall indemnify and hold harmless the Procuring Entity, its officers, employees, and agents from and against any and all claims, losses, damages, liabilities, and expenses arising from:

(a) Breach of contract by the Supplier

(b) Negligent or willful acts of the Supplier's personnel

(c) Infringement of intellectual property rights

(d) Data breaches attributable to the Supplier

(e) Non-compliance with applicable laws and regulations

ARTICLE XI — FORCE MAJEURE

Section 11.1 — Definition

Neither party shall be liable for failure to perform obligations under this Contract due to events beyond reasonable control, including but not limited to: natural disasters, war, terrorism, epidemic or pandemic, government actions, and infrastructure failures not attributable to either party.

Section 11.2 — Notification

The affected party shall notify the other party in writing within FORTY-EIGHT (48) HOURS of the occurrence of a force majeure event, with supporting evidence.

Section 11.3 — Duration

If a force majeure event continues for more than NINETY (90) calendar days, either party may terminate this Contract without penalty, subject to payment for goods delivered and services rendered prior to the force majeure event.

ARTICLE XII — TERMINATION

Section 12.1 — Termination for Convenience

The Procuring Entity may terminate this Contract at any time for its convenience by giving the Supplier SIXTY (60) calendar days written notice. The Supplier shall be entitled to payment for:
(a) Goods delivered and accepted
(b) Services rendered up to the termination date
(c) Reasonable demobilization costs, not to exceed 5% of the remaining contract value

Section 12.2 — Termination for Default

The Procuring Entity may terminate this Contract for default if:

(a) The Supplier fails to deliver goods within the contractual period plus any approved extensions

(b) The Supplier fails to perform any material obligation under this Contract and fails to cure within thirty (30) calendar days of written notice

(c) The Supplier is declared bankrupt or insolvent

(d) The Supplier engages in corrupt, fraudulent, collusive, or coercive practices

Section 12.3 — Effects of Termination for Default

Upon termination for default:

(a) The performance security shall be forfeited

(b) The Supplier shall be blacklisted from government procurement for a period determined by the Government Procurement Policy Board

(c) The Procuring Entity may procure replacement goods and services, with any excess cost charged to the Supplier

ARTICLE XIII — DISPUTE RESOLUTION

Section 13.1 — Amicable Settlement

The parties shall endeavor to settle any dispute arising from this Contract amicably through mutual consultation within THIRTY (30) calendar days of written notice of the dispute.

Section 13.2 — Mediation

If amicable settlement fails, the dispute shall be submitted to mediation under the Philippine Dispute Resolution Center (PDRC) within FIFTEEN (15) calendar days.

Section 13.3 — Arbitration

If mediation fails within SIXTY (60) calendar days, the dispute shall be finally settled by arbitration under the rules of the Philippine Dispute Resolution Center. The arbitration shall be conducted in Quezon City, Philippines, and the language shall be English. The arbitral award shall be final and binding.

Section 13.4 — Governing Law

This Contract shall be governed by and construed in accordance with the laws of the Republic of the Philippines.

ARTICLE XIV — GENERAL PROVISIONS

Section 14.1 — Performance Security

The Supplier shall post a performance security equivalent to FIVE PERCENT (5%) of the total contract price (PHP 2,425,000.00) in the form of:

(a) Cash, cashier's check, or manager's check

(b) Bank guarantee from a reputable bank

(c) Surety bond from a GSIS-accredited surety company

The performance security shall be valid for the duration of the Contract plus six (6) months.

Section 14.2 — Contract Amendments

Any amendment to this Contract shall be in writing and signed by both parties. No amendment shall be valid unless approved by the Head of the Procuring Entity.

Section 14.3 — Assignment and Subcontracting

The Supplier shall not assign or subcontract any portion of this Contract without the prior written consent of the Procuring Entity. Any approved subcontractor shall be bound by the same terms and conditions of this Contract.

Section 14.4 — Notices

All notices under this Contract shall be in writing and delivered to:

For the Procuring Entity:
Director, IT Infrastructure Division
Department of Information and Communications Technology
C.P. Garcia Avenue, Diliman, Quezon City 1101
Email: procurement@dict.gov.ph

For the Supplier:
Vice President, Government Accounts
Pacific Digital Solutions, Inc.
15th Floor, Pacific Star Building
Makati Avenue corner Gil Puyat Avenue, Makati City 1226
Email: government@pacificdigital.com.ph

Section 14.5 — Entire Agreement

This Contract, together with all Annexes, constitutes the entire agreement between the parties and supersedes all prior negotiations, representations, and agreements.

Section 14.6 — Severability

If any provision of this Contract is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

Section 14.7 — Waiver

Failure by either party to enforce any provision of this Contract shall not constitute a waiver of the right to enforce such provision in the future.

ANNEX A

TECHNICAL SPECIFICATIONS SUMMARY

Item 1: Enterprise Rack Servers (40 units)

- Processor: Intel Xeon Gold 6448Y (32 cores, 2.1GHz base)
- Memory: 512GB DDR5-4800 ECC (16x 32GB DIMMs)
- Storage: 4x 1.92TB NVMe SSD (RAID-10)
- Network: 2x 25GbE SFP28 + 1x 1GbE management
- Power: Dual redundant 1400W PSU
- Form Factor: 1U rack mount
- Operating System: Enterprise Linux (3-year subscription)

Item 2: Network Switches (10 units)

- Ports: 48x 25GbE SFP28 + 8x 100GbE QSFP28
- Switching Capacity: 12.8 Tbps
- Managed, Layer 3, stackable (up to 8 units)
- Features: VLAN, QoS, LACP, SNMP v3, sFlow

Item 3: Enterprise Firewalls (5 units)

- Throughput: 40 Gbps (firewall), 20 Gbps (IPS)
- Features: IPS/IDS, SSL inspection, application control
- VPN: 10,000 concurrent IPsec tunnels
- High Availability: Active-Active clustering

Item 4: Storage Arrays (2 units)

- Usable Capacity: 500TB per unit
- Protocol: NVMe-oF, iSCSI, FC 32Gbps
- IOPS: 2,000,000 (4K random read)
- Data Services: Deduplication, compression, snapshots

- Replication: Synchronous between Primary and DR sites

Item 5: UPS Systems (20 units)

- Capacity: 10kVA / 10kW
- Topology: Online double-conversion
- Runtime: 15 minutes at full load (with standard battery)
- Management: SNMP network card included

ANNEX B

SERVICE REQUIREMENTS SUMMARY

1. Network Operations Center (NOC)

- 24/7/365 monitoring of all infrastructure components
- Real-time alerting via email, SMS, and dashboard
- Monthly uptime reporting with root cause analysis
- Staffing: Minimum 2 NOC engineers on duty at all times

2. Helpdesk Support

- Tier 1: First-call resolution for common issues
- Tier 2: Technical troubleshooting and escalation
- Tier 3: Expert-level resolution, vendor coordination
- Ticketing system with SLA tracking
- User satisfaction surveys (target: 90% satisfaction)

3. Security Services

- Monthly vulnerability scanning (all internet-facing systems)
- Quarterly penetration testing
- Annual security audit and compliance assessment
- Incident response team (4-hour mobilization)

4. Backup and Recovery

- Daily incremental backups
- Weekly full backups
- Monthly backup restoration testing
- Recovery Point Objective (RPO): 4 hours

- Recovery Time Objective (RTO): 8 hours

ANNEX C

TRAINING PLAN SUMMARY

Training Program 1: System Administration

- Duration: 5 days (40 hours)
- Participants: 10 DICT system administrators
- Topics: Server management, storage administration, backup operations, monitoring tools, security hardening

Training Program 2: Network Administration

- Duration: 3 days (24 hours)
- Participants: 8 DICT network engineers
- Topics: Switch configuration, firewall management, VPN setup, network monitoring, troubleshooting

Training Program 3: End-User Training

- Duration: 2 days (16 hours)
- Participants: 50 DICT end users
- Topics: Service desk portal, password management, basic troubleshooting, security awareness

Training Program 4: Management Dashboard

- Duration: 1 day (8 hours)
- Participants: 5 DICT managers
- Topics: SLA dashboard, reporting tools, escalation procedures

ANNEX D

MIGRATION PLAN SUMMARY

Phase 1: Assessment (10 days)

- Inventory of existing systems and data
- Data mapping and transformation requirements

- Risk assessment and mitigation plan

Phase 2: Preparation (15 days)

- Setup of migration tools and staging environment
- Development of data transformation scripts
- Creation of rollback procedures

Phase 3: Migration Execution (10 days)

- Incremental data migration (non-critical first)
- Critical system migration (scheduled maintenance window)
- DNS and network cutover

Phase 4: Validation (10 days)

- Data integrity verification
- Application functionality testing
- Performance benchmarking
- User acceptance testing

ANNEX E

PRICING BREAKDOWN (DETAILED)

Hardware:

40x Rack Servers @ PHP 550,000 = PHP 22,000,000.00

10x Network Switches @ PHP 380,000 = PHP 3,800,000.00

5x Firewalls @ PHP 520,000 = PHP 2,600,000.00

2x Storage Arrays @ PHP 1,500,000 = PHP 3,000,000.00

20x UPS Systems @ PHP 37,500 = PHP 750,000.00

Hardware Subtotal: = PHP 32,150,000.00

Software:

Virtualization (40 hosts, 3yr): = PHP 2,800,000.00

Monitoring Suite (3yr): = PHP 1,200,000.00

Backup Solution (3yr): = PHP 1,600,000.00

Endpoint Protection (500 seats, 3yr): = PHP 1,200,000.00

Software Subtotal: = PHP 6,800,000.00

Services:

Managed Services (36 months): = PHP 7,200,000.00

Training (4 programs): = PHP 1,350,000.00

Data Migration: = PHP 1,000,000.00

Services Subtotal: = PHP 9,550,000.00

■■

GRAND TOTAL: = PHP 48,500,000.00

■■

ANNEX F

COMPLIANCE REQUIREMENTS

The Supplier certifies compliance with the following:

1. Republic Act No. 9184 (Government Procurement Reform Act)
2. Republic Act No. 10173 (Data Privacy Act of 2012)
3. Republic Act No. 10175 (Cybercrime Prevention Act of 2012)
4. DICT Department Circular No. 003-2023 (Cloud First Policy)
5. National Privacy Commission Circular No. 2016-01 (Security of Personal Data in Government Agencies)
6. ISO/IEC 27001:2022 (Information Security Management)
7. ISO/IEC 20000-1:2018 (IT Service Management)

ANNEX G -- ACCEPTANCE TESTING PROTOCOL

Section G.1 -- Purpose and Scope

This Annex establishes the comprehensive acceptance testing protocol that the Supplier must satisfy before the Procuring Entity issues a Certificate of Final Acceptance for each deliverable under this Contract. All tests shall be conducted at the Procuring Entity's designated site unless

otherwise agreed in writing.

Section G.2 -- Testing Phases

G.2.1 Factory Acceptance Test (FAT)

The Supplier shall conduct a Factory Acceptance Test at its own facility no later than fifteen (15) calendar days before the scheduled delivery date. The Procuring Entity reserves the right to witness the FAT and shall be given at least ten (10) business days' advance notice.

G.2.2 Site Acceptance Test (SAT)

Upon delivery and physical installation, the Supplier shall perform a Site Acceptance Test within five (5) business days. The SAT shall verify:

(a) Physical integrity of all equipment after transport

(b) Power-on self-test (POST) success for each unit

(c) Firmware and BIOS versions match the approved baseline

(d) Network interface connectivity at the specified link speed

(e) Storage subsystem recognition and health status

G.2.3 Integration Test

Following successful SAT, an Integration Test shall be conducted over a period not exceeding ten (10) business days. This phase verifies interoperability between newly delivered equipment and the Procuring Entity's existing infrastructure, including:

(a) Active Directory domain join and Group Policy application

(b) VLAN assignment and IP addressing per Annex H network plan

(c) DNS resolution of internal and external resources

(d) NTP synchronization with the Procuring Entity's time servers

(e) Backup agent installation and successful test backup/restore

(f) Endpoint protection agent deployment and policy compliance

(g) SIEM log forwarding and event correlation validation

(h) Print queue connectivity and test print verification

G.2.4 Performance and Stress Test

After the Integration Test, a Performance and Stress Test lasting five (5) business days shall be executed. The following metrics must be achieved:

- Server CPU utilization under synthetic load: not to exceed 75% sustained for 30 minutes
- Memory utilization under load: not to exceed 80%
- Disk I/O throughput: minimum 500 MB/s sequential read, 350 MB/s sequential write for SSD-based storage
- Network throughput: minimum 950 Mbps on 1 GbE links; minimum 9.2 Gbps on 10 GbE links
- Application response time: less than 200 ms for standard CRUD operations on the procurement management system
- Database query performance: 95th percentile query time below 50 ms for indexed queries

G.2.5 Security Validation Test

A dedicated security validation shall cover:

(a) Vulnerability scan using an industry-standard scanner (e.g., Nessus, Qualys) with zero critical or high findings

(b) Penetration test of externally facing services -- report to be provided by a CREST-certified assessor

(c) Verification of disk encryption (BitLocker/LUKS) on all endpoints and servers containing sensitive data

(d) Multi-factor authentication enforcement for administrative access to all infrastructure components

(e) Firewall rule review against the approved security baseline

(f) Wireless security audit (WPA3-Enterprise, 802.1X RADIUS)

G.2.6 User Acceptance Test (UAT)

The Procuring Entity shall designate a UAT team of no fewer than ten (10) representative end-users. The UAT period shall be ten (10) business days. Acceptance criteria include:

(a) Successful login and profile setup

(b) Access to all assigned network resources and applications

(c) Printing, scanning, and peripheral functionality

(d) VPN remote access connectivity

(e) Email and collaboration tools (Microsoft 365 / Google Workspace)

(f) Line-of-business application performance satisfaction survey

with a minimum score of 4.0/5.0

Section G.3 -- Test Case Summary

The following table summarizes the minimum required test cases per phase:

Phase Min. Test Cases Pass Rate Required

Factory Acceptance Test 25 100%

Site Acceptance Test 40 100%

Integration Test 60 98%

Performance & Stress Test 30 95%

Security Validation Test 42 100%

User Acceptance Test 50 90%

TOTAL 247

Section G.4 -- Defect Classification

Defects discovered during testing shall be classified as follows:

Severity Description Resolution SLA

Critical System crash, data loss, security 4 hours

breach, or complete service outage

High Major feature failure affecting 8 hours

more than 25% of users

Medium Partial feature failure or 3 business days

significant performance degradation

Low Cosmetic issues, minor UI defects, 10 business days

or non-critical documentation gaps

No Critical or High defects may remain unresolved at the time of Final Acceptance. Medium defects must have a confirmed remediation plan. Low defects may be deferred to the warranty period.

Section G.5 -- Test Environment Requirements

G.5.1 The Supplier shall provide all test tools, scripts, and licenses required for FAT and SAT at no additional cost.

G.5.2 The Procuring Entity shall provide:

(a) Physical space and power for equipment staging

(b) Network connectivity to the test VLAN

(c) Active Directory test accounts (minimum 50)

(d) Access to the staging instance of the procurement system

(e) Designated points of contact for each division

G.5.3 Test data shall be anonymized. No production personal data shall be used in testing without prior written approval from the Data Protection Officer.

Section G.6 -- Reporting and Documentation

G.6.1 The Supplier shall deliver the following test reports:

(a) FAT Report -- within 3 business days of FAT completion

(b) SAT Report -- within 2 business days of SAT completion

(c) Integration Test Report -- within 5 business days

(d) Performance Test Report -- within 5 business days

(e) Security Validation Report -- within 7 business days

(f) UAT Summary Report -- within 5 business days of UAT close

G.6.2 Each report shall include:

- Test scope and objectives

- Test environment description

- Detailed test case results (pass/fail/skip)
- Defect log with classification and resolution status
- Evidence (screenshots, logs, metric dashboards)
- Sign-off section for both parties

Section G.7 -- Re-Test Procedures

Should any test phase fail to meet the required pass rate, the Supplier shall remediate all identified defects and submit a corrective action report within five (5) business days. A re-test shall be scheduled no later than ten (10) business days after the corrective action report is accepted. The Supplier shall bear all costs associated with re-testing.

If a test phase fails three (3) consecutive times, the Procuring Entity may invoke the termination provisions under Article XII of this Contract.

ANNEX H -- NETWORK ARCHITECTURE AND INFRASTRUCTURE DESIGN

Section H.1 -- Overview

This Annex defines the target network architecture for the IT infrastructure being procured under this Contract. The design follows a three-tier collapsed-core topology suitable for the Procuring Entity's headquarters facility.

Section H.2 -- Physical Topology

H.2.1 Core/Distribution Layer

- Two (2) Layer 3 switches in a Virtual Switching System (VSS) or equivalent redundancy configuration
- Minimum 10 GbE uplinks to each access-layer switch
- Dual power supplies with separate UPS feeds
- Stacking or chassis-based design for zero-downtime upgrades

H.2.2 Access Layer

- One (1) 48-port PoE+ Gigabit Ethernet switch per floor
- 802.3at PoE budget of at least 740W per switch
- 2 x 10 GbE uplinks to core in a LAG configuration
- 802.1X port-based authentication on all user ports
- DHCP snooping, Dynamic ARP Inspection, IP Source Guard enabled

H.2.3 Wireless Infrastructure

- Wi-Fi 6E (802.11ax) access points, minimum one per 150 sqm
- Centralized wireless controller with automatic RF management
- Minimum three SSIDs: Corporate, Guest, IoT
- WPA3-Enterprise with 802.1X RADIUS on Corporate SSID
- Captive portal with SMS OTP on Guest SSID
- MAC-based authentication with dedicated VLAN for IoT SSID
- Minimum aggregate throughput of 2.4 Gbps per access point

H.2.4 Server Infrastructure

- Dedicated 10 GbE server VLAN with jumbo frame support (MTU 9000)
- iSCSI or FC-based storage network (separate VLAN or physical fabric)
- Out-of-band management network (IPMI/iLO/iDRAC) on isolated VLAN
- Redundant paths to each server via dual-homed NIC teaming

Section H.3 -- VLAN Design

The following VLAN allocation shall be implemented:

VLAN ID Name Subnet Gateway

---

10 MGMT 10.1.10.0/24 10.1.10.1

20 SERVERS 10.1.20.0/24 10.1.20.1

30 STORAGE 10.1.30.0/24 10.1.30.1

40 VOIP 10.1.40.0/24 10.1.40.1

50 PRINTERS 10.1.50.0/24 10.1.50.1

100 CORP-USERS-F1 10.1.100.0/23 10.1.100.1

102 CORP-USERS-F2 10.1.102.0/23 10.1.102.1

104 CORP-USERS-F3 10.1.104.0/23 10.1.104.1

200 WIFI-CORP 10.1.200.0/23 10.1.200.1

210 WIFI-GUEST 172.16.210.0/23 172.16.210.1

220 WIFI-IOT 172.16.220.0/24 172.16.220.1

250 DMZ 10.1.250.0/28 10.1.250.1

999 QUARANTINE 10.1.255.0/24 10.1.255.1

Section H.4 -- Firewall Zones and Policies

H.4.1 Zone Definitions

Zone Name VLANs Included Trust Level

TRUST 10, 20, 30, 40, 50 High

USER 100, 102, 104 Medium

WIFI-CORP 200 Medium

WIFI-GUEST 210 Low

IOT 220 Low

DMZ 250 Low

INTERNET WAN interfaces Untrusted

H.4.2 Inter-Zone Policy Summary

Source Destination Action Conditions

USER SERVERS Allow Authenticated users, app ports

USER INTERNET Allow Via web proxy, URL filtering

USER DMZ Allow HTTP/HTTPS only

WIFI-CORP SERVERS Allow Same as USER zone

WIFI-CORP INTERNET Allow Via web proxy

WIFI-GUEST INTERNET Allow HTTP/HTTPS/DNS only, rate-limited

WIFI-GUEST Any internal Deny All traffic blocked

IOT SERVERS Allow Specific IoT service ports only

IOT INTERNET Allow Vendor update URLs whitelisted

DMZ SERVERS Allow Specific backend service ports

DMZ INTERNET Allow Outbound HTTPS for APIs

INTERNET DMZ Allow Published services (443, 8443)

INTERNET Any internal Deny All other traffic blocked

MGMT Any Allow Admin access from management net

Any QUARANTINE Redirect NAC policy violation

Section H.5 -- Routing Protocol

H.5.1 Interior Gateway Protocol

- OSPF (Open Shortest Path First) shall be used for interior routing across all Layer 3 devices
- OSPF Area 0 (backbone) for core switches
- OSPF Area 1 for user access networks
- OSPF Area 2 for DMZ and external-facing services
- Passive interfaces on all non-routing VLANs
- Authentication: MD5 or SHA-256 on all OSPF adjacencies

H.5.2 Default Route and WAN

- Dual WAN links: primary fiber (100 Mbps dedicated) and secondary DSL (50 Mbps) for failover
- BGP with ISP for primary link; static default route for backup
- Policy-based routing for traffic engineering
- WAN failover time: less than 30 seconds

Section H.6 -- DNS Architecture

Server Role IP Address Location

Primary Internal DNS 10.1.20.10 Server VLAN

Secondary Internal DNS 10.1.20.11 Server VLAN

DNS Forwarder 10.1.250.5 DMZ

External Authoritative ISP-managed Cloud

- Internal zones: dict.gov.ph (internal), 1.10.in-addr.arpa
- Split-horizon DNS for internal/external resolution
- DNSSEC validation enabled on all resolvers
- DNS query logging forwarded to SIEM

Section H.7 -- NTP and Time Synchronization

Stratum Source IP Address

---

1 Philippine Standard Time (PAGASA) 203.0.113.10

2 Primary NTP Server (on-premise) 10.1.20.15

2 Secondary NTP Server 10.1.20.16

3 All infrastructure devices Sync from Stratum 2

3 All endpoints Sync from Stratum 2

- NTP authentication (symmetric key) on all infrastructure devices
- Maximum allowable drift: 100 milliseconds
- Monitoring alert if drift exceeds 500 milliseconds

Section H.8 -- Quality of Service (QoS)

Traffic Class DSCP Marking Bandwidth Guarantee Queue Priority

---

Voice (VoIP) EF (46) 20% Strict Priority

Video AF41 (34) 15% High

Business Apps AF31 (26) 30% Medium

Default/Web BE (0) 25% Normal

Bulk/Backup AF11 (10) 10% Low

- QoS policies applied at access-layer switch ports
- WAN QoS with traffic shaping on the edge router

- Wireless Multimedia (WMM) enabled on all SSIDs

Section H.9 -- Network Monitoring

H.9.1 The following monitoring tools shall be deployed:

(a) SNMP v3 polling of all network devices (5-minute intervals)

(b) NetFlow/sFlow collection for traffic analysis

(c) Syslog aggregation to centralized SIEM

(d) Automated configuration backup (daily)

(e) Uptime monitoring with 1-minute ping intervals

(f) Bandwidth utilization dashboards per VLAN

H.9.2 Alert Thresholds

Metric Warning Critical

CPU Utilization 70% 90%

Memory Utilization 75% 90%

Link Utilization 60% 80%

Packet Loss 0.1% 1.0%

Interface Errors 100/hr 1000/hr

Section H.10 -- IP Address Management (IPAM)

- Centralized IPAM solution integrated with DNS and DHCP

- All static assignments documented in IPAM database

- DHCP lease time: 8 hours for wired, 4 hours for wireless

- DHCP failover between primary and secondary servers

- Reserved ranges in each subnet:

.1-.10 Network infrastructure (gateways, switches)

.11-.20 Servers and critical services

.21-.50 Static assignments (printers, APs, cameras)

.51-.254 DHCP dynamic pool

ANNEX I -- DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

Section I.1 -- Objectives

This Annex defines the Disaster Recovery (DR) and Business Continuity Plan (BCP) requirements for the IT infrastructure and services delivered under this Contract. The Supplier shall design, implement, and support DR/BCP capabilities that meet the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified herein.

Section I.2 -- Recovery Objectives by Service Tier

Service Tier RTO RPO Examples

Tier 1 1 hour 15 minutes Email, procurement system,

(Mission financial database, DNS,

Critical) Active Directory

Tier 2 4 hours 1 hour Document management, HR

(Business information system, intranet

Essential) portal, print services

Tier 3 24 hours 4 hours Training platform, analytics

(Standard) dashboards, development and

test environments

Tier 4 72 hours 24 hours Archive systems, legacy

(Deferrable) applications, non-critical

file shares

Section I.3 -- Backup Strategy

I.3.1 Backup Schedule

Data Type Full Backup Incremental Retention

System Images Weekly (Sun) Daily 90 days

Databases Daily Every 4 hrs 180 days

File Shares Weekly (Sat) Daily 365 days

Email Archives Monthly Daily 7 years

Configuration On change N/A Unlimited

Logs (SIEM) N/A Continuous 365 days

I.3.2 Backup Media and Storage

(a) Primary backup to on-premise disk-based backup appliance with minimum 50 TB usable capacity

(b) Secondary copy to offsite location via encrypted WAN link (AES-256 encryption in transit and at rest)

(c) Monthly tape backup to fireproof vault for long-term retention (email archives, financial records)

(d) Cloud backup for Tier 1 services to government-approved cloud provider (must comply with DICT cloud-first policy)

I.3.3 Backup Verification

- Daily automated restore test of a random database backup
- Weekly automated restore test of a random file share
- Monthly full system image restore to isolated test environment
- Quarterly DR drill with documented results

Section I.4 -- Failover Scenarios

The following failover scenarios shall be supported:

I.4.1 Single Server Failure

- Automated failover via hypervisor high availability (HA)
- VM restart on surviving host within 5 minutes
- No data loss (shared storage)
- No manual intervention required

I.4.2 Storage Array Failure

- Synchronous replication to secondary array
- Automatic path failover via multipath I/O
- RPO: zero data loss
- RTO: less than 2 minutes

I.4.3 Network Switch Failure (Core)

- VSS/VPC automatic failover to redundant core switch
- Convergence time: less than 3 seconds
- No user-perceptible outage for established sessions

I.4.4 Network Switch Failure (Access)

- Manual replacement from on-site spare inventory
- Pre-configured spare with automated config restore
- Target RTO: 30 minutes
- Users on affected floor may use wireless as interim

I.4.5 WAN Link Failure (Primary)

- Automatic failover to secondary WAN link
- BGP path withdrawal and reconvergence: less than 60 seconds
- Reduced bandwidth during failover (50 Mbps vs 100 Mbps)
- Non-critical traffic deprioritized via QoS policies

I.4.6 Power Failure (Partial)

- UPS sustains critical load for 30 minutes minimum
- Generator auto-start within 15 seconds of utility loss
- Graceful shutdown of non-critical systems if generator fails
- PDU-level monitoring and automatic load shedding

I.4.7 Power Failure (Complete/Extended)

- All Tier 1 services fail over to DR site
- Tier 2 services restored within 4 hours at DR site
- Staff switch to remote work using VPN and cloud services
- Communication via mobile phones and personal hotspots

I.4.8 Cooling System Failure

- Temperature sensors trigger alert at 28 degrees Celsius
- Critical alert and automatic workload migration at 32 degrees
- Emergency shutdown at 38 degrees to prevent hardware damage
- Portable cooling units deployed from facilities management

I.4.9 Ransomware/Cyber Attack

- Immediate network isolation of affected segments
- Activation of clean backup from air-gapped media
- Forensic investigation by incident response team
- Restoration priority per service tier classification
- Estimated full recovery: 24-72 hours depending on scope

I.4.10 Physical Disaster (Fire/Flood/Earthquake)

- Full activation of DR site
- All services restored per tier-based RTO
- Staff relocation to alternate work site
- Estimated full recovery: 24-96 hours

Section I.5 -- DR Site Requirements

I.5.1 The DR site shall be located at least fifty (50) kilometers from the primary site but within Metro Manila or nearby provinces for accessibility.

I.5.2 The DR site shall maintain:

(a) Replica of all Tier 1 server infrastructure (active-passive)

(b) Network connectivity to primary site via dedicated link

(c) Independent internet connectivity (different ISP)

(d) Independent power supply with UPS and generator

(e) Physical security equivalent to the primary site

(f) Environmental controls (cooling, fire suppression)

(g) Minimum 10 workstations for essential staff

I.5.3 Data replication between sites:

- Tier 1: Synchronous replication (zero RPO)
- Tier 2: Asynchronous replication (15-minute RPO)

- Tier 3: Daily backup copy transfer
- Tier 4: Weekly backup copy transfer

Section I.6 -- DR Testing Schedule

Test Type Frequency Duration Participants

Tabletop Exercise Quarterly 2 hours IT staff + mgmt

Component Failover Monthly 1 hour IT operations

Partial DR Activation Semi-annual 4 hours IT + key users

Full DR Activation Annual 8 hours All stakeholders

Surprise DR Drill Annual 4 hours IT operations

Section I.7 -- Roles and Responsibilities During DR

Role Primary Contact Alternate

DR Commander CIO Deputy CIO

IT Operations Lead IT Director Senior SysAdmin

Network Lead Network Manager Network Engineer

Database Lead DBA Manager Senior DBA

Application Lead App Dev Manager Senior Developer

Security Lead CISO Security Analyst

Communications Lead PR Director Comms Manager

Facilities Lead Admin Director Facilities Mgr

Vendor Liaison Procurement Head Contract Manager

ANNEX J -- SECURITY AND COMPLIANCE MATRIX

Section J.1 -- Purpose

This Annex provides a comprehensive security and compliance matrix mapping the requirements of this Contract to applicable Philippine laws, international standards, and industry best practices.

Section J.2 -- Regulatory Compliance Matrix

Requirement RA 9184 RA 10173 RA 10175 DICT CC

Data classification -- Sec 20 -- 4.2

Privacy impact assessment -- Sec 21 -- 4.3

Consent management -- Sec 12 -- --

Breach notification -- Sec 20(f) Sec 7 4.7

Data retention schedule -- Sec 11 -- 4.5

Procurement transparency Sec 3 -- -- --

Bid evaluation criteria Sec 30 -- -- --

Contract performance review Sec 37 -- -- --

Cybercrime prevention -- -- Sec 4-10 4.8

Government cloud policy -- -- -- 5.1

Legend:

RA 9184 = Government Procurement Reform Act

RA 10173 = Data Privacy Act of 2012

RA 10175 = Cybercrime Prevention Act of 2012

DICT CC = DICT Circular No. 003-2023

Section J.3 -- ISO 27001:2022 Control Mapping

ISO Control Description Implementation Status

A.5.1 Information security policies Required - Day 1

A.5.2 Information security roles Required - Day 1

A.5.3 Segregation of duties Required - Day 30

A.6.1 Screening Required - Pre-deploy

A.6.2 Terms of employment Required - Pre-deploy

A.6.3 Information security awareness Required - Day 60

A.7.1 Physical security perimeters Required - Day 1

A.7.2 Physical entry controls Required - Day 1

A.7.3 Securing offices and rooms Required - Day 1

A.7.4 Physical security monitoring Required - Day 30

A.7.5 Protection against threats Required - Day 1

A.7.6 Working in secure areas Required - Day 1

A.7.7 Clear desk and clear screen Required - Day 30

A.7.8 Equipment siting and protection Required - Day 1

A.7.9 Security of assets off-premises Required - Day 30

A.7.10 Storage media Required - Day 1

A.7.11 Supporting utilities Required - Day 1

A.7.12 Cabling security Required - Day 1

A.7.13 Equipment maintenance Required - Day 30

A.7.14 Secure disposal/re-use Required - Day 1

A.8.1 User endpoint devices Required - Day 1

A.8.2 Privileged access rights Required - Day 1

A.8.3 Information access restriction Required - Day 1

A.8.4 Access to source code Required - Day 30

A.8.5 Secure authentication Required - Day 1

A.8.6 Capacity management Required - Day 30

A.8.7 Protection against malware Required - Day 1

A.8.8 Mgmt of technical vulnerabilities Required - Day 30

A.8.9 Configuration management Required - Day 30

A.8.10 Information deletion Required - Day 60

A.8.11 Data masking Required - Day 60

A.8.12 Data leakage prevention Required - Day 60

A.8.13 Information backup Required - Day 1

A.8.14 Redundancy of info processing Required - Day 1

A.8.15 Logging Required - Day 1

A.8.16 Monitoring activities Required - Day 30

A.8.17 Clock synchronization Required - Day 1

A.8.18 Use of privileged utility programs Required - Day 1

A.8.19 Install of software on ops systems Required - Day 1

A.8.20 Networks security Required - Day 1

A.8.21 Security of network services Required - Day 1

A.8.22 Segregation of networks Required - Day 1

A.8.23 Web filtering Required - Day 30

A.8.24 Use of cryptography Required - Day 1

A.8.25 Secure development life cycle Required - Day 60

A.8.26 Application security requirements Required - Day 60

A.8.27 Secure system architecture Required - Day 1

A.8.28 Secure coding Required - Day 60

Section J.4 -- Security Baseline Requirements

J.4.1 Endpoint Security

(a) All endpoints shall have enterprise antivirus/EDR installed

(b) Host-based firewall enabled with deny-by-default policy

(c) Full disk encryption (BitLocker for Windows, LUKS for Linux)

(d) USB storage disabled by default via Group Policy

(e) Application whitelisting on high-security workstations

(f) Automatic screen lock after 5 minutes of inactivity

(g) Local administrator account disabled; admin access via PAM

(h) Software installation restricted to IT-approved channels

J.4.2 Server Security

(a) Hardened OS image per CIS Benchmark Level 2

(b) Only required services and ports enabled

(c) Administrative access via jump server (bastion host) only

(d) SSH key-based authentication; password auth disabled

(e) File integrity monitoring on critical system files

(f) Security patches applied within 72 hours (critical) or

30 days (non-critical)

(g) Centralized log collection to SIEM (retain 365 days)

(h) Database encryption at rest for sensitive data

J.4.3 Network Security

(a) Next-generation firewall with IPS, application control, and SSL/TLS inspection

(b) Network segmentation per Annex H VLAN design

(c) 802.1X network access control on all wired ports

(d) Wireless intrusion detection and prevention system (WIDS/WIPS)

(e) DNS sinkhole for known malicious domains

(f) Web proxy with URL categorization and SSL inspection

(g) Email security gateway with anti-spam, anti-phishing, sandboxing, and DMARC/DKIM/SPF enforcement

(h) DDoS mitigation at the ISP level

J.4.4 Identity and Access Management

(a) Centralized identity provider (Active Directory or equivalent)

(b) Multi-factor authentication for all administrative access

(c) MFA for all remote access (VPN, web applications)

(d) Role-based access control (RBAC) with quarterly review

(e) Privileged Access Management (PAM) solution for admin accounts

(f) Password policy: minimum 12 characters, complexity required, 90-day rotation, 24-password history

(g) Account lockout after 5 failed attempts (30-minute lockout)

(h) Automated de-provisioning within 24 hours of termination

J.4.5 Security Operations

(a) Security Information and Event Management (SIEM) deployment

(b) 24x7 security monitoring (SOC) -- may be outsourced

(c) Incident response plan with defined escalation procedures

(d) Vulnerability scanning -- monthly internal, quarterly external

(e) Penetration testing -- annual, by independent assessor

(f) Security awareness training -- quarterly for all staff

(g) Phishing simulation -- monthly, with metrics reporting

(h) Threat intelligence feed integration with SIEM and firewall

Section J.5 -- Data Classification Framework

Classification Description Handling Requirements

TOP SECRET National security data, Encrypted at rest and classified government info in transit, need-to-know access only, no cloud

CONFIDENTIAL Personal data, financial Encrypted at rest and records, procurement in transit, role-based evaluations, salary data access, audit logging

INTERNAL Internal communications, Access restricted to policies, procedures, employees, no external meeting minutes sharing without approval

PUBLIC Press releases, published No special handling reports, public-facing required website content

---

Section J.6 -- Incident Response Procedures

J.6.1 Incident Classification

Category Description Response Time

P1 Active breach, data exfiltration 15 minutes

P2 Malware outbreak, ransomware 30 minutes

P3 Policy violation, unauthorized 2 hours access attempt

P4 Suspicious activity, anomaly 4 hours

P5 Security inquiry, false positive Next business day

J.6.2 Incident Response Phases

(a) Detection and Analysis

- Alert triage by SOC analyst
- Initial classification and severity assessment
- Evidence preservation (memory dumps, disk images, logs)

(b) Containment

- Network isolation of affected systems
- Account suspension for compromised credentials
- Temporary firewall rules to block attack vectors

(c) Eradication

- Malware removal and system cleaning
- Vulnerability patching
- Password resets for affected accounts

(d) Recovery

- System restoration from clean backups
- Gradual reconnection with monitoring
- User communication and access restoration

(e) Post-Incident

- Root cause analysis within 5 business days
- Lessons learned report
- Policy and procedure updates
- NPC notification within 72 hours if personal data affected

Section J.7 -- Audit and Compliance Reporting

Report Frequency Audience

Security Posture Dashboard Real-time CISO, CIO

Vulnerability Scan Report Monthly IT Security Team

Access Review Report Quarterly Department Heads, HR

Compliance Status Report Quarterly Management Committee

Penetration Test Report Annual CIO, CISO, External Auditor

SIEM Summary Report Monthly IT Security Team

Incident Summary Report Monthly CISO, CIO

Data Privacy Impact Review Annual DPO, NPC

Third-Party Risk Assessment Annual Procurement, CISO

ANNEX K -- CHANGE MANAGEMENT PROCEDURES

Section K.1 -- Purpose

This Annex establishes the change management framework governing all modifications to the IT infrastructure and services delivered under this Contract. The objective is to ensure that changes are implemented in a controlled manner with minimum disruption to service.

Section K.2 -- Change Categories

Category Description Approval Required

Standard Pre-approved, low-risk, routine Change Manager only
(e.g., password resets, patch
deployment per schedule)

Normal Planned changes with moderate Change Advisory Board
risk (e.g., new server deploy, (CAB)
VLAN modification, firewall rule)

Emergency Unplanned changes to resolve Emergency CAB (2 members
critical incidents or security minimum, verbal approval
vulnerabilities acceptable, documented
within 24 hours)

Section K.3 -- Change Advisory Board (CAB)

K.3.1 Composition

- Chairperson: IT Director (Procuring Entity)

- Members:

(a) Network Manager

(b) System Administrator Team Lead

(c) Database Administrator

(d) Information Security Officer

(e) Supplier's Project Manager

(f) Supplier's Technical Lead

(g) Representative from affected business unit (as needed)

K.3.2 Meeting Schedule

- Regular CAB: Every Wednesday, 2:00 PM - 3:30 PM

- Emergency CAB: Convened within 30 minutes of emergency request

K.3.3 Quorum: Minimum 4 members including the Chairperson or designated alternate.

Section K.4 -- Change Request Process

K.4.1 Submission

- All change requests submitted via the IT Service Management (ITSM) tool at least 5 business days before planned implementation

- Emergency changes may be submitted verbally and documented within 24 hours

K.4.2 Required Information

(a) Change description and justification

(b) Risk assessment (impact and likelihood)

(c) Affected systems and services

(d) Implementation plan with step-by-step procedures

(e) Rollback plan with step-by-step procedures

(f) Testing plan and expected results

(g) Resource requirements (personnel, downtime, budget)

(h) Communication plan (who needs to be notified)

(i) Scheduled implementation window

K.4.3 Review and Approval

- Standard changes: Reviewed by Change Manager within 1 business day
- Normal changes: Reviewed at next CAB meeting
- Emergency changes: Reviewed by Emergency CAB within 30 minutes

K.4.4 Implementation

- Changes implemented during approved maintenance windows:
* Primary window: Saturday 10:00 PM - Sunday 6:00 AM
* Secondary window: Wednesday 10:00 PM - Thursday 4:00 AM
- Emergency changes may be implemented outside maintenance windows
- Implementation monitored by Change Manager or designee

K.4.5 Post-Implementation Review

- Verification testing within 2 hours of implementation
- Change record updated with results
- Failed changes trigger immediate rollback
- Post-implementation review at next CAB meeting

Section K.5 -- Change Risk Assessment Matrix

Impact High Medium Low

High Critical High Medium

Likelihood (Exec. (CAB + (CAB

Sponsor Business approval)

approval) Owner)

Medium High Medium Low

(CAB + (CAB (Change

Business approval) Manager)

Owner)

Low Medium Low Standard

(CAB (Change (Pre-approved)

approval) Manager)

Section K.6 -- Maintenance Windows and Blackout Periods

K.6.1 Standard Maintenance Windows

- Weekly: Saturday 10:00 PM to Sunday 6:00 AM
- Monthly: Last Saturday of month, 6:00 PM to Sunday 12:00 PM
- Quarterly: Aligned with system update schedule

K.6.2 Blackout Periods (No changes except emergency)

- Month-end close: Last 3 business days of each month
- Year-end close: December 15 to January 5
- Audit periods: As communicated by Finance/COA
- Election periods: As mandated by COMELEC
- National disaster response activations

Section K.7 -- Key Performance Indicators

KPI Target Measurement

Change success rate 95% Monthly

Unauthorized changes 0 Monthly

Emergency change ratio < 10% Monthly

Change-related incidents < 5% Monthly

Average lead time (normal) < 7 days Monthly

Rollback success rate 100% Per occurrence

CAB meeting attendance > 80% Monthly

Post-implementation review rate 100% Monthly

ANNEX L -- DATA PROCESSING AGREEMENT

Section L.1 -- Parties and Definitions

This Data Processing Agreement (DPA) is entered into by and between the Procuring Entity (as Data Controller) and the Supplier (as Data

Processor) in accordance with Republic Act No. 10173 (Data Privacy Act of 2012), its Implementing Rules and Regulations, and applicable issuances of the National Privacy Commission (NPC).

L.1.1 Definitions

(a) "Personal Data" -- any information from which the identity of an individual can be reasonably and directly ascertained, or when put together with other information would directly and certainly identify an individual

(b) "Sensitive Personal Information" -- personal data about an individual's race, marital status, age, religious or political affiliations, health, education, genetic or sexual life, proceedings for any offense, government-issued IDs, or specifically established by law as classified

(c) "Data Subject" -- the individual whose personal data is processed

(d) "Processing" -- any operation performed on personal data including collection, recording, organization, storage, updating, retrieval, consultation, use, consolidation, blocking, erasure, or destruction

Section L.2 -- Scope of Processing

L.2.1 Categories of Data Subjects

(a) Employees of the Procuring Entity

(b) Contractors and consultants

(c) Citizens and stakeholders interacting with government services

(d) Supplier's personnel assigned to the Contract

L.2.2 Types of Personal Data Processed

(a) Contact information (name, address, email, phone number)

(b) Employment information (employee ID, position, department)

(c) Government-issued identification numbers (TIN, SSS, PhilHealth, Pag-IBIG, GSIS)

(d) Financial information (bank account details for payroll)

(e) IT usage data (login records, access logs, email metadata)

(f) CCTV footage from monitored areas

L.2.3 Purpose of Processing

The Supplier processes personal data solely for the purpose of delivering the IT infrastructure and managed services specified in this Contract, including:

(a) System administration and user account management

(b) Technical support and incident resolution

(c) Security monitoring and incident response

(d) Backup and disaster recovery operations

(e) Performance monitoring and capacity planning

(f) Reporting and compliance activities

Section L.3 -- Obligations of the Data Processor (Supplier)

L.3.1 The Supplier shall:

(a) Process personal data only upon documented instructions from the Procuring Entity

(b) Ensure that personnel authorized to process personal data have committed to confidentiality

(c) Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including as appropriate:

- Pseudonymization and encryption of personal data
- Ability to ensure confidentiality, integrity, availability, and resilience of processing systems
- Ability to restore availability and access to personal data in a timely manner in the event of an incident
- Regular testing and evaluation of security measures

(d) Not engage another processor without prior written authorization from the Procuring Entity

(e) Assist the Procuring Entity in responding to data subject

requests (access, correction, erasure, portability)

(f) Delete or return all personal data upon termination of the Contract, at the Procuring Entity's election

(g) Make available all information necessary to demonstrate compliance with this DPA and allow for audits

Section L.4 -- Sub-Processing

L.4.1 The Supplier shall not subcontract any processing activities without prior written consent of the Procuring Entity.

L.4.2 Where sub-processing is authorized, the Supplier shall:

(a) Impose the same data protection obligations as this DPA

(b) Remain fully liable for the sub-processor's performance

(c) Maintain a current register of sub-processors

(d) Notify the Procuring Entity of any intended changes to sub-processors at least 30 days in advance

L.4.3 Currently Authorized Sub-Processors:

Sub-Processor Service Location

CloudSecure PH, Inc. Cloud backup Manila, PH

NetWatch Solutions SOC monitoring Cebu, PH

Section L.5 -- Data Breach Notification

L.5.1 The Supplier shall notify the Procuring Entity of any personal data breach without undue delay and in any event within twelve (12) hours of becoming aware of the breach.

L.5.2 The notification shall include:

(a) Description of the nature of the breach

(b) Categories and approximate number of data subjects affected

(c) Categories and approximate number of records affected

(d) Likely consequences of the breach

(e) Measures taken or proposed to address the breach

(f) Contact details of the Supplier's Data Protection Officer

L.5.3 The Procuring Entity shall notify the NPC and affected data subjects within seventy-two (72) hours of being informed of the breach, as required by NPC Circular 16-03.

Section L.6 -- Data Transfer and Location

L.6.1 All personal data shall be stored and processed within the territory of the Republic of the Philippines.

L.6.2 No personal data shall be transferred outside the Philippines without prior written authorization from the Procuring Entity and compliance with the requirements of Section 21 of RA 10173.

L.6.3 Data center locations for this Contract:

Facility Location Classification

Primary DC Quezon City, PH Tier III

DR Site Laguna, PH Tier II+

Backup Vault Makati City, PH Tier II

Section L.7 -- Data Retention and Disposal

L.7.1 Personal data shall be retained only for the duration necessary to fulfill the purposes of processing.

L.7.2 Retention Schedule

Data Category Retention Period Disposal Method

Active employee records Duration of Secure deletion

employment + 5 yrs (NIST 800-88)

Former employee records 5 years from Secure deletion

separation

System access logs 1 year Automated purge

CCTV footage 90 days Automated overwrite

Incident reports 3 years Secure deletion

Backup tapes (long-term) 7 years Degaussing + shred

L.7.3 Upon contract termination, the Supplier shall:

(a) Return all personal data in a standard, machine-readable format within 30 calendar days

(b) Securely delete all copies from the Supplier's systems within 60 calendar days

(c) Provide a certificate of destruction signed by an authorized officer

Section L.8 -- Audit Rights

L.8.1 The Procuring Entity may conduct audits of the Supplier's data processing activities with 15 business days' notice.

L.8.2 The Procuring Entity may engage an independent third-party auditor, subject to confidentiality obligations.

L.8.3 The Supplier shall cooperate fully with any audit and provide access to facilities, systems, records, and personnel.

L.8.4 Audit frequency shall not exceed twice per calendar year unless a data breach or compliance concern warrants additional review.

Section L.9 -- Liability and Indemnification

L.9.1 The Supplier shall indemnify the Procuring Entity against any losses, damages, claims, or penalties arising from the Supplier's breach of this DPA or applicable data privacy laws.

L.9.2 The Supplier shall maintain cyber liability insurance with a

minimum coverage of PHP 50,000,000.00 (Fifty Million Pesos) for the duration of this Contract.

L.9.3 Penalties for DPA violations:

(a) First violation: Written warning + corrective action plan

(b) Second violation: PHP 500,000 penalty + enhanced monitoring

(c) Third violation: Grounds for contract termination under Article XII + NPC complaint referral

Section L.10 -- Term and Survival

L.10.1 This DPA shall remain in effect for the duration of the Contract and for an additional period of five (5) years after termination for obligations relating to data retention, disposal, and confidentiality.

L.10.2 Sections L.5 (Breach Notification), L.7 (Retention and Disposal), L.8 (Audit Rights), and L.9 (Liability) shall survive the termination of this DPA.

SIGNATURE PAGE

IN WITNESS WHEREOF, the parties have hereunto set their hands this 15th day of January 2025 at Quezon City, Philippines.

FOR THE PROCURING ENTITY: FOR THE SUPPLIER:

_____ _____

HON. MARIA ELENA C. SANTOS MR. ROBERTO A. VILLAROSA

Secretary, DICT President & CEO

Pacific Digital Solutions, Inc.

WITNESSES:

_____ _____

ATTY. JOSE P. REYES MS. CARLA B. MENDOZA

Chief of Staff, DICT VP, Government Accounts

Pacific Digital Solutions, Inc.

ACKNOWLEDGED BY:

_____

ATTY. RAMON L. GARCIA

Head, BAC Secretariat, DICT