TERMS OF REFERENCE

Corrective Maintenance and Support for Active Directory Domain Services (ADDS) and Active Directory Certificate Services (ADCS)

Version

Version	Date	Status	Author
1	23/10/2026	Final	ITSD

Terms of Reference

Corrective Maintenance and Support for Active Directory Domain Services (ADDS) and Active Directory Certificate Services (ADCS)

I. Background

The ASEAN Secretariat (ASEC) was established in February 1976 by the Foreign Ministers of ASEAN. It is currently staffed with approximately 450 people, with the mission to initiate, facilitate, and coordinate collaboration among ASEAN stakeholders to achieve the purposes and principles of ASEAN, as outlined in the ASEAN Charter. To fulfill its mandate of ensuring efficient coordination among ASEAN organs and effective implementation of ASEAN programs and initiatives, ASEC continuously strives to enhance its operational efficiency and internal processes.

ASEC utilises Active Directory Domain Services (ADDS) and Active Directory Certificate Services (ADCS) as essential components of its IT infrastructure. ADDS provides centralised user authentication, identity and access management, and directory services, while ADCS supports the issuance and management of digital certificates required for secure authentication and communication. These services play a critical role in supporting ASEC's day-to-day IT operations and various systems and applications, including user access to network resources, corporate applications, and other services that rely on Active Directory authentication and digital certificates.

Given the critical role of ADDS and ADCS in supporting ASEC's IT operations, any disruption or technical issues affecting these services could potentially impact the availability and accessibility of dependent systems and applications. To ensure the continued reliability and availability of these services, ASEC requires specialised technical support to address and resolve technical issues related to ADDS and ADCS. The provision of corrective maintenance and support services is therefore essential to facilitate timely troubleshooting and resolution of incidents, minimise potential service downtime, and reduce disruptions to ASEC's daily operations.

II. Objectives

To ensure the continued reliability and availability of ASEC’s Active Directory Domain Services (ADDS) and Active Directory Certificate Services (ADCS) through the provision of specialised corrective maintenance and technical support services. These services aim to facilitate timely troubleshooting and resolution of technical issues, minimise potential service downtime, and reduce disruptions to ASEC’s IT operations and dependent systems and applications.

III. Expected Deliverables

The selected vendor shall provide corrective maintenance and technical support services for ASEC's Active Directory Domain Services (ADDS) and Active Directory Certificate Services (ADCS) on an as-needed basis throughout the contract period. The expected deliverables include:

1. The vendor shall provide corrective maintenance, troubleshooting, and service recovery support for reported technical issues affecting ADDS and ADCS, in accordance with the agreed scope of services and Service Level Agreement (SLA).
2. The vendor shall submit a corrective maintenance report upon completion of each support activity, including detailing the reported issue, root cause where identified, troubleshooting performed, corrective actions taken, resolution status and recommendations to prevent recurrence.
3. The vendor shall submit bi-annual reports summarising support incidents logs and utilisation of support hours, including any outstanding issues, if any.

IV. Scope of Services

The vendor shall provide corrective maintenance and technical support for ASEC's Active Directory Domain Services (ADDS) and Active Directory Certificate Services (ADCS) on an as-needed basis, in accordance with the agreed Service Level Agreement (SLA).

The scope of services shall cover four (4) ADDS servers and one (1) ADCS server, comprising three (3) ADDS servers and one (1) ADCS server hosted on-premises and running Windows Server 2019 and one (1) ADDS server hosted on Microsoft Azure running Windows Server 2022.

The scope of services shall include the following:

a. Active Directory Domain Services (ADDS) Corrective Maintenance and Support

i. Diagnose, troubleshoot, and resolve technical issues affecting ADDS, including Active Directory replication failures, domain authentication and logon issues, and Group Policy processing failures.
ii. Provide troubleshooting and service recovery support for Domain Controller failures and Microsoft DNS issues directly affecting ADDS operations.
iii. Troubleshoot Kerberos authentication and time synchronisation issues originating from the ADDS environment.
iv. Provide troubleshooting support for ADDS-related issues affecting authentication and access to dependent enterprise applications and services, limited to the ADDS components.

b. Active Directory Certificate Services (ADCS) Corrective Maintenance and Support

i. Diagnose, troubleshoot, and resolve technical issues affecting ADCS, including Certificate Authority (CA) service failures, particularly in connection with ASEC's Corporate System using on-premise Microsoft Dynamics 365
ii. Provide troubleshooting and restoration assistance for CA database corruption, subject to the availability and integrity of ASEC-maintained backups.
iii. Troubleshoot certificate-related issues originating from ADCS, including certificate issuance

and renewal, Certificate Revocation List (CRL) publication, certificate trust chain, and certificate validation failures.

iv. Provide restoration assistance for ADCS services following hardware failure, limited to the ADCS role and associated Windows Server operating system, on an operational replacement platform provided by ASEC.

c. Corrective Maintenance for ADDS and ADCS arising from Security Incidents, Operating System Upgrades, Server Migrations, or other related activities

i. Provide technical assistance for the recovery of ADDS or ADCS services affected by cybersecurity incidents, including malware or ransomware attacks.

ii. Assist in restoring affected ADDS or ADCS services using available backups and a suitably secured recovery environment provided by ASEC.

iii. Provide troubleshooting for Windows Server operating system issues directly affecting ADDS or ADCS services, including issues arising from operating system patch updates.

iv. Provide troubleshooting and service recovery assistance for ADDS or ADCS configuration issues arising from server migration or operating system upgrades performed by ASEC or its appointed personnel.

d. Technical Support Channels and Reporting

i. Provide telephone and email for problem escalation and remote assistance, and able to deliver Remote Support for fast resolution.

ii. Where necessary, facilitate escalation to Microsoft, subject to the availability of applicable Microsoft support entitlements.

iii. Provide a dedicated support contact person to coordinate support requests, incident resolution, and service-related communications with ASEC.

iv. Submit a corrective maintenance report upon completion of each corrective maintenance activity, including the reported issue, troubleshooting performed, corrective actions taken, and resolution status.

v. Submit bi-annually reports summarising logged support incidents and utilisation of the contracted support hours.

e. Service Period and Support Man-Hours

i. The vendor shall provide a total of 120 man-hours of corrective maintenance and support services for a period of twelve (12) months, from 1 December 2026 until 30 November 2027.

ii. Vendor shall provide rate per hour for each additional man-hour should additional support hours be required beyond the allocated 120 man-hours. For this instance, the vendor shall submit a quotation for ASEC's review and approval prior to the provision of additional services.

iii. Any unused support hours may, subject to mutual agreement between ASEC and the vendor, be utilised for ADDS and ADCS-related advisory services, including configuration reviews, optimisation recommendations, security hardening guidance, certificate dependency assessment and technical consultation.

V. Services Exclusion

The following activities are not part of the scope of service:

i. Preventive maintenance, continuous monitoring, routine system administration, and housekeeping activities.
ii. System upgrades, operating system migrations, new implementations, or expansion of existing services.
iii. Routine patch deployment, patch management, and rollback execution.
iv. Hardware, storage, virtualisation, network infrastructure, and cloud platform support.
v. Third-party application troubleshooting, application code remediation, and end-user device support, except where the issue is identified as originating from the supported ADDS or ADCS environment.
vi. Cybersecurity incident response activities, including threat containment, forensic investigation, malware removal, threat hunting, and security monitoring.
vii. General DNS, such as application-specific DNS, network DNS, third-party DNS etc. related issues are excluded unless ADDS is identified as the contributing Microsoft platform component.
viii. Any products that have reached the End of Extended Support lifecycle by Microsoft, it shall be supported on a best-effort basis.

VI. Service Level Agreement

Severity	High	Medium	Low
Response Time	<1 hours (during business hours) <2 hours (during nonbusiness hours)	<4 hours	<6 hours
Resolution Time*	The resolution or workaround time is targeted as 4 hours (after issue escalation) and should it get extended, vendor will commit to continuous operation in extended hours (24x7) until the resolution.	The resolution or workaround time is targeted as 8 hours (after issue escalation) and should it get extended, vendor will commit to continuous operation daily (8:00 a.m. to 6:00 p.m.) until the resolution.	The resolution or workaround time is targeted as 12 hours (after issue escalation) and should it get extended, vendor will commit to continuous operation Monday to Friday (8:00 a.m. to 6:00 p.m.) until the resolution.

* ASEC's relevant technical personnel will work closely with the vendor throughout the troubleshooting and resolution process until the issue is resolved.

Severity Classification

- High: Total outage of ADDS or ADCS services, or service degradation or disruption affecting more than 50% of users
- Medium: Service degradation or disruption affecting between 10% - 50% of users

- Low: Service degradation or disruption affecting less than 10% of users

Service Window:

- Overall Service Coverage: 24 hours a day, 7 days a week (24×7).
- Business Hours: Monday to Friday, 8:00 a.m. to 6:00 p.m. Western Indonesia Time (WIB).
- Non-Business Hours: Emergency technical support, as required, outside normal business hours, including weekends and public holidays.

VII. Penalty

For problem resolution beyond the agreed SLA, a penalty of 0.5% of the contract fee for each hour beyond the SLA resolution time will be imposed, capped at a maximum of 10% of contracted value.

VIII. Vendor Qualification

The vendor shall demonstrate following expertise and qualifications:

1. An established company with at least 5 years of proven experience in providing technical support, troubleshooting, and maintenance services for Microsoft Active Directory Domain Services (ADDS) and Active Directory Certificate Services (ADCS) for government agencies, multinational companies, international organisations, or similar institutions.

2. Technical person assigned should have at least 5 years of experience in supporting Microsoft Active Directory environments hosted on both on-premises infrastructure and Microsoft Azure as well as experience in supporting Active Directory Certificate Services (ADCS).

3. Technical personnel assigned shall possess good written and verbal communication skills in English.

4. Vendor should be a Microsoft Solution partner.

*****