BPJS Kesehatan
Badan Penyelenggara Jaminan Sosial

PENGUMUMAN TENDER DENGAN PENILAIAN TEKNIS
PENGADAAN JASA MANAGED SECURITY SERVICE PROVIDER

Nomor : 03/PTMSSP/1125

Diumumkan bahwa BPJS Kesehatan Kantor Pusat akan melaksanakan Tender Dengan Penilaian Teknis untuk Pengadaan Jasa *Managed Security Service Provider*, dengan ketentuan sebagai berikut:

1. Pelaku Usaha yang berminat mengikuti Tender ini harus terdaftar sebagai Daftar Penyedia Terkualifikasi BPJS Kesehatan.
2. Apabila Pelaku Usaha belum terdaftar sebagai Penyedia Terkualifikasi di BPJS Kesehatan, agar Pelaku Usaha melakukan Pendaftaran Calon Penyedia BPJS Kesehatan, yaitu melakukan registrasi *online* melalui **website** **https://procurement.bpjs-kesehatan.go.id**, melakukan pengisian data, menyerahkan dokumen administrasi dan melakukan verifikasi keaslian dokumen administrasi.
3. Ruang lingkup pekerjaan Tender Dengan Penilaian Teknis untuk Pengadaan Jasa *Managed Security Service Provider* sebagaimana lampiran 1.
4. Pendaftaran dan Pengambilan Dokumen Tender
   a. Dibuka Tanggal : Jumat, 7 November 2025 jam 08.00 WIB
   b. Ditutup Tanggal : Senin, 17 November 2025 jam 16.00 WIB
   c. Tempat : BPJS Kesehatan Kantor Pusat
   Kedeputian Bidang SDS & Umum (Gd. Rizali Noor Lantai 7)
   Jl. Letjen Suprapto Kav.20 No.14 Cempaka Putih
   Jakarta Pusat (Pendaftaran & pengambilan dokumen Tender bisa mengubungi Sdr. Rifky terlebih dahulu melalui email panitia.tender@bpjs-kesehatan.go.id)
5. Pendaftaran Tender dilakukan dengan persyaratan sebagai berikut:
   a. Terdaftar sebagai Daftar Penyedia Terkualifikasi (DPT) BPJS Kesehatan, dibuktikan dengan *Print out* sertifikat BPJS Kesehatan dengan **status aktif**.
   b. Asli Surat Pendaftaran keikutsertaan Tender Dengan Penilaian Teknis Pengadaan Jasa *Managed Security Service Provider*.
   c. Asli Surat Kuasa pendaftaran dari Pimpinan Perusahaan (Direksi atau Kepala Cabang Perusahaan) apabila yang mendaftar bukan Pimpinan Perusahaan.
   d. Fotokopi SIUP/NIB 62029 bidang Aktivitas Konsultasi Komputer dan Manajemen Fasilitas Komputer Lainnya atau 62090 bidang Aktivitas Teknologi Informasi dan Jasa Komputer Lainnya atau 62019 bidang Aktivitas Pemrograman Komputer Lainnya atau 63112 bidang Aktivitas Hosting dan YBDI atau 63111 bdiang Aktivitas Pengolahan Data dengan kualifikasi Menengah (M) atau Besar (B) yang masih berlaku.
   (ASLI SIUP DIPERLIHATKAN SAAT PENDAFTARAN)
   e. Fotokopi sertifikasi ISO 27001

Kantor Pusat
Jl. Letjen Suprapto Kav. 20 No.14, Cempaka Putih
PO BOX 1391/JKT, Jakarta Pusat 10510 - Indonesia
Telp. +62 21 421 2938 (Hunting), Fax. +62 21 421 2940
www.bpjs-kesehatan.go.id

f. Memiliki Pengalaman Kerja Pengadaan IT Security/sejenis dalam kurun waktu 3 (tiga) tahun terakhir dengan nilai total kumulatif minimal sebesar Rp.1.000.000.000,00 (Satu Miliar Rupiah) untuk total keseluruhan Perjanjian Kerjasama/Kontrak/Surat Pesanan/PO. Fotokopi Perjanjian Kerja Sama/Kontrak/Surat Pesanan yang disampaikan harus lengkap (melampirkan ruang lingkup pekerjaan atau spesifikasi teknis dan nilai pekerjaan) **(Asli Perjanjian Kerjasama/Kontrak diperlihatkan saat pendaftaran).**

g. Fotokopi Neraca Perusahaan dan Laporan Laba Rugi Perusahaan tahun 2024 yang telah diaudit Akuntan Publik (KAP) berikut opininya, yaitu Wajar yang dikeluarkan oleh Kantor Akuntan Publik.

   Apabila saat ini belum atau sedang proses Audit oleh KAP, maka melampirkan:

   1) Fotokopi Surat keterangan sedang proses audit dari KAP apabila sedang dalam proses audit atau Surat Pernyataan Pimpinan Perusahaan bahwa belum Proses Audit;
   2) Fotokopi Neraca Perusahaan dan Laba Rugi Perusahaan Tahun 2023 yang telah diaudit Akuntan Publik dengan opini Wajar
   3) Asli Neraca Perusahaan Tahun 2024 *Unaudited* yang ditandatangani oleh Pimpinan Perusahaan;
   4) Asli Laba Rugi Perusahaan Tahun 2024 *Unaudited* yang ditandatangani oleh Pimpinan Perusahaan.

      (Asli Neraca Perusahaan dan Laporan Laba Rugi Perusahaan yang telah diaudit Akuntan Publik (KAP) diperlihatkan saat pendaftaran)

h. Fotokopi Bukti Pajak Badan Tahun 2024/2023, adapun bukti pajak badan meliputi:

   1) Bukti Penerimaan Surat SPT Tahunan PPh Wajib Pajak Badan Tahun 2024/2023;
   2) SPT Tahunan PPh Wajib Pajak Badan Tahun 2024/2023 (dapat secara manual atau elektronik); dan
   3) Surat Setoran Pajak (SSP) Tahun 2024/2023, apabila kurang bayar (dapat secara manual atau elektronik).

      (ASLI PAJAK BADAN DIPERLIHATKAN SAAT PENDAFTARAN)

i. Asli Surat Pernyataan bermeterai ditandatangani oleh Pimpinan Perusahaan yang menandatangani Surat Permohonan sebagai Calon Peserta Tender yang menyatakan:

   1) Memiliki kemampuan menyediakan fasilitas, peralatan dan personil yang diperlukan untuk pelaksanaan pekerjaan dimaksud.
   2) Bahwa dokumen-dokumen yang disampaikan adalah benar.
   3) Bahwa tidak dalam pengawasan pengadilan, tidak dalam proses hukum, tidak bangkrut, kegiatan usahanya tidak sedang dihentikan dan/atau tidak sedang menjalani sanksi pidana.
   4) Bahwa Perusahaannya telah mendaftarkan seluruh pekerjanya sebagai Peserta JKN KIS BPJS Kesehatan (mencantumkan nomor *Virtual Account* BPJS Kesehatan dan dibuktikan dengan fotokopi bukti pembayaran iuran JKN KIS BPJS Kesehatan minimal bulan Oktober 2025).

j. Asli Pakta Integritas diketik di atas kertas kop perusahaan, diberi tanggal, bermeterai, ditandatangani oleh Pimpinan Perusahaan dan diberi cap perusahaan sesuai format sebagaimana lampiran 2.

Jakarta, 7 November 2025
Panitia Tender
BPJS Kesehatan Kantor Pusat

Lampiran 1 Pengumuman Tender
Nomor : 03/PTMSSP/1125
Tanggal 7 November 2025

RINCIAN BIAYA, RUANG LINGKUP DAN SPESIFIKASI TEKNIS,
PENGADAAN JASA MANAGED SECURITY SERVICE PROVIDER

A. RINCIAN BIAYA

1. Biaya Pekerjaan Tier 1 dan Tier 2

No	Item	Qty	Satuan	Harga (Rp)
a	b	c	d	e
1	Tier 1	1	Paket	-
2	Tier 2	1	Paket	-
Total Harga Sebelum PPN				-
DPP PPN (11/12 x Harga Sebelum PPN)				-
PPN (12% x DPP PPN)				-
Total Harga Setelah PPN				-

2. Biaya Pekerjaan Tier 3

No	Item	Satuan	Harga (Rp)
a	b	c	d
1	Tier 3	Per Server	-
Total Harga Sebelum PPN			-
DPP PPN (11/12 x Harga Sebelum PPN)			-
PPN (12% x DPP PPN)			-
Total Harga Setelah PPN			-

B. RUANG LINGKUP PEKERJAAN

Ruang Lingkup Pekerjaan Pengadaan Jasa Managed Security Service Provider adalah sebagai berikut:

1. Pekerjaan Tier 1 adalah jasa managed security service provider atas pekerjaan event monitoring and analysis dengan ruang lingkup pekerjaan, rincian dan spesifikasi sebagai berikut :

   Menyediakan minimal 8 orang engineer on-site selama 24 jam 7 hari dan setiap shift beranggotakan 2 orang tenaga ahli, dengan ruang lingkup sebagai berikut:

   a. Melakukan monitoring alert, memberikan informasi alert dan analisa potensi risiko yang diperoleh dari seluruh perangkat keamanan yang dimiliki BPJS Kesehatan yang telah terintegrasi pada Security Orchestration, Automation and Response (SOAR). Dalam kondisi perangkat keamanan belum terintegrasi secara keseluruhan dengan SOAR maka Tim Tier 1 melakukan monitoring alert dan analisis terhadap perangkat tersebut secara terpisah, tidak terbatas pada perangkat Security Information and Event Management (SIEM), Sandbox,

Endpoint Detection and Response (EDR), Network Detection and Response (NDR), Data Loss Prevention (DLP), Threat Intelligence Platform Management, Mail Security, Mobile Application Security, Vulnerability Management, maksimal 15 menit sejak alert muncul.

b. Melakukan tindakan pengamanan terhadap jenis alert yang telah ditentukan langkah tindak lanjutnya maksimal 30 menit sejak alert muncul.
c. Melakukan pencatatan security register dari kegiatan monitoring dan analisis di setiap akhir shift.
d. Melakukan monitoring dan memberikan informasi status perangkat SOAR setiap awal shift dan melakukan backup log pada perangkat SIEM atau perangkat keamanan lainnya di BPJS Kesehatan sesuai dengan kebutuhan.
e. Melakukan vulnerability assesment terhadap aplikasi publik BPJS Kesehatan, melakukan analisa dan penilaian risiko terhadap temuan ketidaksesuaian hasil asesmen dan memberikan rekomendasi kepada BPJS Kesehatan minimal 1x per bulan.
f. Memberikan analisis ancaman dan kerentanan serta memberikan saran dan rekomendasi berkaitan masalah kerentanan keamanan yang relevan dengan BPJS Kesehatan ketika ada isu cyber security yang muncul.

2. Pekerjaan Tier 2 adalah jasa managed security service provider atas pekerjaan Event Correlation and Investigation dengan ruang lingkup pekerjaan, rincian dan spesifikasi sebagai berikut :

   Menyediakan minimal 1 orang engineer on-site yang berbedadengan personil Tier 1 selama 8 jam kerja pada hari kerja (senin-jumat) dan on-call diluar jam kerja dan hari kerja, dengan ruang lingkup sebagai berikut:

   a. Melakukan analisis, identifikasi dan tindaklanjut untuk mengisolir atau menahan serangan terhadap alert/event maksimal 1 jam setelah alert muncul.
   b. Melakukan pencarian dan eliminasi terhadap akar masalah dari alert/insiden yang telah terjadi maksimal 1 jam setelah alert muncul.
   c. Menginformasikan hasil analisa dan tindaklanjut terhadap event dan alert kepada Tim BPJS Kesehatan maksimal 15 menit setelah analisa dilakukan.
   d. Melakukan simulasi serangan siber (teknis) kepada tim Security Incident Response Team untuk meningkatkan kemampuan tim dalam menangani dan menganalisis insiden minimal 1x per tahun.
   e. Melakukan review dan memberikan rekomendasi peningkatan efektivitas aturan, kebijakan atau policy dalam sistem dan perangkat keamanan dan jaringan minimal 1x per bulan.
   f. Melakukan analisis dan evaluasi terhadap konfigurasi perangkat keamanan dalam rangka meningkatkan fungsionalitas pemantauan, deteksi, analisa dan visibility terhadap seluruh data minimal 1x per bulan.

3. Pekerjaan Tier 3 adalah jasa managed security service provider atas pekerjaan Digital Forensic and Incident Response dengan ruang lingkup pekerjaan, rincian dan spesifikasi sebagai berikut :

   Jasa untuk Digital Forensic dan Incident Response hanya digunakan ketika terjadi insiden dan membutuhkan pekerjaan digital forensic secara mendalam dengan

personil yang berbeda dengan personil Tier 1 dan Tier 2, dengan ruang lingkup sebagai berikut:

a. Melakukan respon dan menganalisa risiko serta dampak dari setiap kejadian insiden yang di eskalasi dari tim Tier 2.
b. Melakukan forensik digital, investigasi kronologi kejadian, melakukan analisis malware dan reverse engineering pada aset terdampak sesuai dengan kategorinya.
c. Melakukan analisa strategi dan rencana penanganan serta rekomendasi pemulihan pasca terjadinya insiden.
d. Memberikan rekomendasi untuk tim Tier 2 guna peningkatan pendeteksian ancaman, serta rekomendasi paska penanggulanan insiden.
e. Berperan sebagai Subject Matter Expert (SME) dalam proses identifikasi, proteksi, deteksi, respon dan recovery insiden.
f. Melakukan koordinasi bersama tim terkait untuk penanganan insiden yang perlu melibatkan banyak pihak dan pemangku kepentingan.
g. Membuat laporan Root Cause Analysis (RCA) dan memberikan rekomendasi strategis sebagai lesson learn agar insiden serupa tidak terjadi kembali.
h. Insiden akan dituangkan dalam Berita Acara Kesepakatan Penggunaan Jasa Tier 3.

4. Menyediakan tenaga ahli yang dibutuhkan untuk pekerjaan ini sesuai kualifikasi

C. METODE KERJA

Metode kerja yang harus dilakukan penyedia jasa antara lain:

1. Monitoring, melakukan event monitoring selama 24x7 dan menindaklanjuti event sesuai dengan tingkat severity tertentu.
2. Asesmen, melakukan vulnerability assesment terhadap seluruh aplikasi publik BPJS Kesehatan.
3. Optimalisasi konfigurasi perangkat Jaringan dan Keamanan TI

D. LAPORAN KEMAJUAN PEKERJAAN

Laporan laporan yang harus dibuat oleh penyedia jasa antara lain:

1. Tahapan Tier 1
   a. Laporan harian kegiatan monitoring dan tindak lanjut terhadap event yang muncul.
   b. Laporan bulanan Vulnerability Assesment aplikasi publik BPJS Kesehatan.
   c. Laporan harian capture health status perangkat SOAR.
   d. Laporan bulanan yang merupakan gabungan dari seluruh laporan diatas serta seluruh kegiatan monitoring yang dilakukan.
2. Tahapan Tier 2
   a. Laporan hasil analisa dari alert/event yang muncul.
   b. Laporan bulanan rekomendasi optimalisasi policy pada perangkat jaringan dan keamanan TI.
   c. Laporan bulanan hasil asesmen konfigurasi perangkat jaringan dan keamanan TI.
   d. Laporan hasil simulasi serangan siber.

3. Laporan yang harus dibuat oleh penyedia jasa jika Tier 3 dilaksanakan antara lain :
   a. Laporan hasil digital forensik yang meliputi laporan teknis terkait langkah-langkah dan aktifitas yang dilakukan dalam proses forensik.
   b. Laporan rekomendasi perbaikan celah keamanan infrastruktur teknologi informasi dan rencana remediasi.
   c. Laporan rekomendasi prevensi yang perlu dilaksanakan untuk menghindari terulangnya insiden serupa yang disebabkan oleh hal-hal yang telah ditemukan.
   d. Laporan Root Cause Analysis.

Lampiran 2 Pengumuman Tender
Nomor : 03/PTMSSP/1125
Tanggal 7 November 2025

KOP PERUSAHAAN

PAKTA INTEGRITAS

Saya yang bertanda tangan di bawah ini:

Nama	:	...
No. Identitas	:	... *[diisi nomor KTP]*
Jabatan	:	... *[Pimpinan Perusahaan]*
Bertindak untuk dan atas nama	:	PT .../CV .../Firma ...*[diisi sesuai kebutuhan dan cantumkan nama perusahaan]*

dalam rangka Pengadaan Barang/Jasa untuk Pekerjaan Pengadaan **Jasa *Managed Security Service Provider***, dengan ini menyatakan bahwa:

1. Tidak akan melakukan praktik Suap, Korupsi, Kolusi dan Nepotisme (KKN) dengan pegawai/oknum pegawai BPJS Kesehatan atau sesama Penyedia Barang/Jasa dalam proses pengadaan barang/jasa di lingkungan BPJS Kesehatan;
2. Akan melaporkan ke Sistem Pelaporan Pelanggaran *Whistleblowing System* (WBS) BPJS Kesehatan melalui email wbs@bpjs-kesehatan.go.id apabila mengetahui ada indikasi Suap, Gratifikasi, Korupsi, Kolusi, Nepotisme di dalam proses pengadaan ini;
3. Akan mengikuti proses pengadaan barang/jasa secara bersih, transparan, dan profesional untuk memberikan hasil kerja terbaik sesuai ketentuan peraturan perundang-undangan;
4. Menghormati dan mentaati segala keputusan proses Pengadaan Barang/Jasa Pekerjaan **Pengadaan Jasa *Managed Security Service Provider;***
5. Apabila melanggar hal-hal yang dinyatakan dalam PAKTA INTEGRITAS ini, bersedia menerima sanksi administratif, menerima sanksi pencantuman dalam Daftar Hitam, digugat secara perdata dan/atau dilaporkan secara pidana

...[tempat], *…[tanggal] …[bulan] …[tahun]*
[Nama Perusahaan]

[Tanda Tangan dan Cap Perusahaan di atas Meterai]

[Nama Pimpinan Perusahaan]