

**KERANGKA ACUAN KERJA**  
**PENGADAAN EMAIL SECURITY BARRACUDA DAN**  
***LOCAL SUPPORT***



**KLIRING  
BERJANGKA  
INDONESIA**

Member of  **Danareksa**

**PT. KLIRING BERJANGKA INDONESIA**  
**Menara Danareksa Lantai 6**  
**Jl. Medan Merdeka Selatan No 14, Jakarta Pusat**  
**10110 2026**

# Daftar Isi

I	DOCUMENT VERSION .....	3
II	PENDAHULUAN .....	4
2.1	Latar Belakang .....	4
2.2	Maksud dan Tujuan .....	4
III	LINGKUP PEKERJAAN .....	5
3.1	Penyediaan Lisensi .....	5
3.2	Implementasi dan Konfigurasi .....	5
3.3	Integrasi dengan Microsoft 365 .....	6
3.4	Policy Configuration .....	6
3.5	Testing dan UAT .....	6
3.6	Dokumentasi .....	6
3.7	Knowledge Transfer .....	7
3.8	Support dan Maintenance .....	7
IV	SPEKIFIKASI TEKNIS .....	7
4.1	Spesifikasi Umum .....	7
4.2	Fitur Email Security Barracuda .....	7
4.3	Integrasi Email Security Barracuda .....	8
V	DELIVERABLES .....	9
5.1	Deliverable Lisensi .....	9
5.2	Dokumen Teknis .....	9
5.3	Dokumen UAT .....	9
5.4	Materi Transfer Knowledge .....	9
5.5	Laporan Berkala .....	9
VI	JANGKA WAKTU PELAKSANAAN .....	10
VII	KRITERIA DAN KUALIFIKASI VENDOR .....	11
7.1	Kualifikasi Teknis .....	11
7.2	Dokumen yang Harus Dilampirkan .....	11
VIII	SERVICE LEVEL AGREEMENT (SLA) .....	11
8.1.	Klasifikasi Tingkat Insiden .....	11
8.2.	Jam Layanan .....	12

IX	KELUARAN .....	12
9.1	Dokumen Teknis .....	12
9.2	Deliverable Lisensi .....	12
9.3	Laporan Berkala.....	12
9.4	Bukti Kehadiran dan Aktivitas.....	13
X	Timelin Proses Pengadaan.....	13
XI	Harga Perkiraan Sendiri (HPS).....	14
XII	PENUTUP.....	14

## I DOCUMENT VERSION

<b>Versi</b>	<b>Tanggal</b>	<b>Bagian</b>	<b>Jenis Perubahan</b>	<b>Penulis Perubahan</b>
1.0	08 - 5 - 2026	All	Pembuatan Document	Krisna Aji Putra
1.1	11-05-2026	Timeline	Menambahkan timeline proses pengadaan	Rangga Fattaqi Amri
1.2	11-05-2026	Support	Perubahan skema support	Krisna Aji Putra

## II PENDAHULUAN

### 2.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat telah menjadikan email sebagai salah satu media komunikasi bisnis yang paling kritis dalam operasional perusahaan. Ketergantungan yang tinggi terhadap layanan email berbasis cloud, khususnya Microsoft 365 dan *Exchange Online*, membawa konsekuensi peningkatan eksposur terhadap berbagai bentuk ancaman siber yang semakin canggih dan terorganisir.

Ancaman keamanan email terus berkembang dengan tingkat kompleksitas yang signifikan, mencakup serangan phishing yang ditargetkan (*spear phishing*), *Business Email Compromise* (BEC), distribusi malware dan ransomware melalui lampiran email berbahaya, serta eksploitasi tautan URL untuk mengarahkan pengguna ke situs palsu. Berdasarkan laporan keamanan siber global terkini, lebih dari 90% insiden keamanan siber di lingkungan korporasi diawali melalui vektor serangan email.

Meskipun Microsoft 365 telah dilengkapi dengan mekanisme perlindungan email bawaan seperti *Exchange Online Protection* (EOP) dan *Microsoft Defender for Office 365*, fitur-fitur *native* tersebut memiliki keterbatasan dalam menghadapi ancaman siber yang semakin adaptif dan terevolusi. Diperlukan solusi email security tambahan yang mampu memberikan lapisan perlindungan lebih dalam, deteksi ancaman yang lebih akurat, serta kapabilitas respons yang lebih komprehensif.

Pertimbangan kepatuhan (*compliance*) terhadap regulasi keamanan informasi yang berlaku, termasuk kebijakan internal perusahaan, standar internasional ISO/IEC 27001, serta regulasi perlindungan data, juga memperkuat kebutuhan atas solusi email *security* yang terkelola dan terdokumentasi dengan baik.

Berdasarkan pertimbangan-pertimbangan di atas, PT. Kliring Berjangka Indonesia bermaksud melaksanakan pengadaan solusi *Email Security* berbasis *Barracuda* untuk memperkuat postur keamanan komunikasi email perusahaan secara menyeluruh dan berkelanjutan.

### 2.2 Maksud dan Tujuan

Maksud dari pengadaan solusi Email Security Barracuda ini adalah menyediakan platform keamanan email yang terintegrasi, komprehensif, dan terpusat untuk melindungi seluruh ekosistem komunikasi email perusahaan berbasis Microsoft 365 / Exchange Online dari ancaman siber yang semakin kompleks, serta memastikan tersedianya dukungan teknis profesional dari penyedia jasa yang berpengalaman dan tersertifikasi resmi oleh Barracuda Networks.

Tujuan spesifik yang ingin dicapai melalui pengadaan ini meliputi:

- Melindungi layanan email perusahaan berbasis Microsoft 365 dan Exchange Online dari serangan phishing, spear phishing, Business Email Compromise (BEC), malware, ransomware, dan ancaman berbasis email lainnya secara real-time.
- Mengurangi volume spam dan email berbahaya yang masuk ke inbox karyawan secara signifikan, sehingga meningkatkan produktivitas dan mengurangi risiko insiden keamanan akibat kelalaian pengguna.
- Meningkatkan keamanan komunikasi email melalui fitur enkripsi email (Email Encryption) untuk memastikan kerahasiaan informasi sensitif perusahaan dalam transmisi.
- Mengimplementasikan mekanisme monitoring dan filtering email yang terpusat dan terkelola melalui konsol manajemen Barracuda yang terintegrasi penuh dengan Microsoft 365.
- Menambah lapisan keamanan (defense in depth) pada Microsoft 365 yang melampaui kemampuan Microsoft Exchange Online Protection (EOP) bawaan, mencakup analisis ancaman berbasis AI/ML, sandboxing lampiran, dan URL rewriting.
- Mencegah kebocoran data sensitif perusahaan melalui saluran email dengan implementasi Data Loss Prevention (DLP) yang terkoneksi dengan kebijakan keamanan informasi perusahaan.
- Menyederhanakan manajemen karantina email dan respons insiden melalui antarmuka yang intuitif dan terotomatisasi.
- Memastikan kepatuhan (compliance) perusahaan terhadap regulasi perlindungan data dan standar keamanan informasi yang berlaku melalui fitur audit trail, logging, dan pelaporan yang komprehensif.

### III LINGKUP PEKERJAAN

Penyedia jasa yang ditunjuk bertanggung jawab untuk melaksanakan seluruh ruang lingkup pekerjaan berikut:

#### 3.1 Penyediaan Lisensi

- Pengadaan **lisensi Barracuda Email Security ADVANCED for Microsoft 365** jumlah 100 mailbox aktif perusahaan.
- Penjaminan keaslian lisensi yang diperoleh dari Barracuda Networks atau distributor resmi yang ditunjuk.
- Penyerahan dokumen lisensi resmi (License Certificate) beserta bukti aktivasi.
- Notifikasi perpanjangan lisensi minimal 60 (enam puluh) hari sebelum tanggal kadaluarsa.
- Garansi ketersediaan update engine, update definisi ancaman, dan update platform selama masa lisensi aktif.

#### 3.2 Implementasi dan Konfigurasi

- Pelaksanaan asesmen awal (initial assessment) terhadap infrastruktur email Microsoft 365 eksisting, termasuk inventarisasi mailbox, mail flow, dan konfigurasi DNS (MX, SPF, DKIM, DMARC).
- Instalasi dan konfigurasi Barracuda Email Security terintegrasi dengan Microsoft 365 / Exchange Online via API native dan/atau connector.
- Konfigurasi mail flow (SMTP routing) untuk memastikan seluruh email masuk dan keluar diproses melalui platform Barracuda.

- Konfigurasi kebijakan keamanan email (email security policy) sesuai standar dan kebutuhan organisasi.
- Aktivasi dan konfigurasi seluruh modul perlindungan: Anti-Spam, Anti-Phishing, Anti-Malware, URL Protection, Attachment Sandboxing, DLP, Email Encryption, dan Impersonation Protection.
- Konfigurasi manajemen karantina email (Quarantine Management) termasuk notifikasi kepada pengguna.
- Pengaturan role-based access control (RBAC) untuk administrator dan operator konsol.
- Konfigurasi alerting, notifikasi, dan dashboard monitoring.
- Pengujian fungsionalitas komprehensif (end-to-end testing) dan validasi konfigurasi sebelum go-live.
- Penyusunan dokumen konfigurasi (as-built document) sebagai referensi operasional.

### **3.3 Integrasi dengan Microsoft 365**

- Integrasi dengan Azure Active Directory (Azure AD / Entra ID) untuk sinkronisasi pengguna dan manajemen akses.
- Integrasi dengan Exchange Online untuk pengelolaan mail flow, policy enforcement, dan proteksi inbound/outbound.
- Konfigurasi Enhanced Filtering (connectors) pada Exchange Online untuk mempertahankan IP address asli pengirim.
- Integrasi dengan Microsoft Defender for Office 365 (jika tersedia) untuk koordinasi perlindungan berlapis.

### **3.4 Policy Configuration**

- Penyusunan dan penerapan kebijakan anti-spam dengan klasifikasi skor spam yang sesuai.
- Konfigurasi whitelist dan blacklist domain/IP pengirim sesuai perangkat sebelumnya.
- Konfigurasi Policy Keamanan sesuai dengan standard.
- Konfigurasi Impersonation Protection untuk melindungi eksekutif dan domain perusahaan dari serangan BEC.

### **3.5 Testing dan UAT**

- Pengujian skenario phishing simulation untuk memvalidasi efektivitas deteksi.
- Pengujian pengiriman dan penerimaan email normal (legitimate email) untuk memastikan tidak ada false positive yang signifikan.
- User Acceptance Testing (UAT) bersama tim TI dan perwakilan pengguna akhir.
- Dokumentasi hasil UAT dan sign-off formal dari pihak perusahaan.

### **3.6 Dokumentasi**

- Dokumen desain solusi (Solution Design Document / HLD dan LLD).
- Dokumen konfigurasi perangkat (As-Built / MOP Configuration Document).
- Materi transfer knowledge dan panduan pengguna.

### 3.7 Knowledge Transfer

- Pelatihan administrasi konsol Barracuda Email Security untuk operator dan administrator.
- Pelatihan interpretasi log, laporan, dan dashboard keamanan.
- Penyediaan modul pelatihan (slide, dokument guide, dan video tutorial).

### 3.8 Support dan Maintenance

- Layanan dukungan untuk insiden kategori **P1 (Critical)** dan **P2 (High)** tersedia **24x7 (setiap hari dan setiap waktu)**, termasuk di luar jam kerja, hari libur nasional, dan akhir pekan.
- Layanan dukungan untuk insiden kategori **P3 (Medium)** dan **P4 (Low)** tersedia pada **jam kerja (Business Hours)**, yaitu **Senin–Jumat pukul 09.00–18.00 WIB**.
- Preventive Maintenance per 3 bulan mencakup health check, review policy.
- Quarterly Report postur keamanan email setiap 3 (tiga) bulan.
- Eskalasi ke Barracuda Support untuk isu teknis yang memerlukan penanganan principal.

## IV SPESIFIKASI TEKNIS

### 4.1 Spesifikasi Umum

Solusi Email Security yang diadakan wajib memenuhi persyaratan umum sebagai berikut:

- Mendukung integrasi native dengan Microsoft 365 / Exchange Online melalui Microsoft API.
- Berbasis cloud untuk memastikan ketersediaan tinggi (high availability) dan skalabilitas.
- Mendukung perlindungan email inbound dan outbound secara .
- Menyediakan konsol manajemen terpusat yang dapat diakses secara web-based (web console).
- Mendukung multi-domain dan multi-tenant management.
- Menyediakan dashboard real-time, laporan periodik, dan audit log yang komprehensif.
- Memiliki kapabilitas automatic update untuk engine, signature, dan definisi ancaman tanpa memerlukan intervensi manual.

### 4.2 Fitur Email Security Barracuda

Solusi yang ditawarkan wajib mencakup fitur-fitur minimum berikut:

No.	Fitur	Deskripsi
1	Anti-Spam	Filtering email spam menggunakan reputasi IP, analisis header, bayesian filtering, dan machine learning dengan akurasi minimal 99%.
2	Anti-Phishing	Deteksi dan pemblokiran email phishing termasuk spear phishing, credential harvesting, dan domain spoofing berbasis AI.
3	Anti-Malware	Pemindaian lampiran email untuk mendeteksi virus, trojan, ransomware, dan malware lainnya menggunakan multiple scan engine.

No.	Fitur	Deskripsi
4	URL Protection	Pemeriksaan dan rewriting URL dalam badan email secara real-time untuk mendeteksi link berbahaya pada saat diklik (time-of-click protection).
5	Email Encryption	Enkripsi otomatis email outbound yang mengandung informasi sensitif sesuai kebijakan DLP.
6	Quarantine Management	Manajemen karantina email terpusat dengan notifikasi pengguna otomatis dan portal self-service release.
7	Reporting & Monitoring	Dashboard real-time dan laporan periodik mencakup statistik ancaman, mail flow, dan efektivitas filtering.
8	Impersonation Protection	Deteksi dan pemblokiran serangan yang menggunakan identitas eksekutif atau domain perusahaan (CEO fraud, BEC).
9	DMARC/DKIM/SPF Enforcement	Validasi dan enforcement protokol autentikasi email standar untuk mencegah email spoofing.

### 4.3 Integrasi Email Security Barracuda

Solusi wajib mendukung integrasi teknis berikut:

Komponen Integrasi	Keterangan	Protokol / Metode
Azure Active Directory (Entra ID)	Sinkronisasi pengguna, grup, dan domain secara otomatis dari direktori Microsoft 365.	Microsoft Graph API / Azure AD Connector
Exchange Online	Proteksi mail flow inbound dan outbound melalui Exchange Online.	SMTP Connector / API Integration
SMTP Routing	Konfigurasi MX record dan SMTP relay untuk memastikan seluruh email diproses melalui Barracuda.	MX Record, Smart Host, Connector
Microsoft Defender for O365	Koordinasi perlindungan email berlapis jika Defender for O365 telah aktif di tenant Microsoft 365.	Enhanced Filtering / API
SIEM / Log Management	Ekspor log dan alert ke platform SIEM (Security Information & Event Management) yang digunakan perusahaan.	Syslog / API / HTTPS Webhook

## **V DELIVERABLES**

Penyedia jasa wajib menghasilkan dan menyerahkan seluruh deliverable berikut kepada pihak perusahaan:

### **5.1 Deliverable Lisensi**

- Sertifikat Lisensi Resmi **Barracuda Email Security ADVANCE for Microsoft 365** untuk seluruh mailbox terdaftar.
- Bukti aktivasi lisensi yang dapat diverifikasi melalui portal resmi Barracuda Networks.
- Jadwal perpanjangan lisensi dan reminder otomatis kepada perusahaan.

### **5.2 Dokumen Teknis**

- Dokumen Hasil Asesmen Awal: Inventarisasi mailbox, topologi mail flow, konfigurasi DNS, dan kondisi keamanan email eksisting.
- High-Level Design (HLD): Arsitektur solusi Email Security Barracuda dan integrasinya dengan Microsoft 365.
- Low-Level Design (LLD) / Solution Design Document (SDD): Detail teknis konfigurasi, parameter, dan policy yang akan diterapkan.
- As-Built Configuration Document: Dokumentasi seluruh konfigurasi final yang telah diterapkan di lingkungan produksi.

### **5.3 Dokumen UAT**

- Test Plan: Rencana pengujian mencakup skenario, kriteria keberhasilan, dan metode pengujian.
- Test Result Report: Hasil pengujian UAT yang ditandatangani oleh pihak perusahaan dan vendor.
- Berita Acara Serah Terima (BAST) implementasi.

### **5.4 Materi Transfer Knowledge**

- Slide presentasi pelatihan administrasi dan operasional Barracuda Email Security.
- Panduan Operasional (User Guide) dalam Bahasa Indonesia.

### **5.5 Laporan Berkala**

- Laporan Preventive Maintenance: Laporan per 3 bulan mencakup status kesehatan platform, update yang dilakukan, dan temuan.
- Laporan Corrective Maintenance: Laporan penanganan insiden per kejadian beserta root cause analysis.
- Quarterly Report: Laporan komprehensif postur keamanan email setiap 3 (tiga) bulan sekali.
- Laporan Akhir Kontrak: Ringkasan layanan, pencapaian SLA, statistik ancaman, dan rekomendasi untuk periode berikutnya.

## VI JANGKA WAKTU PELAKSANAAN

Jadwal pelaksanaan implementasi Email Security Barracuda adalah sebagai berikut:

No.	Kegiatan	Durasi	Keterangan
1	Kick-off Meeting & Assessment	3 hari kerja	Pertemuan awal, inventarisasi mailbox, review konfigurasi Microsoft 365, dan DNS eksisting.
2	Persiapan Lisensi & Aktivasi	7 hari kerja	Proses pengadaan, aktivasi, dan verifikasi lisensi Barracuda di portal resmi.
3	Desain dan Perencanaan	3 hari kerja	Penyusunan HLD, LLD, dan rencana migrasi/implementasi.
4	Konfigurasi dan Integrasi M365	5 hari kerja	Konfigurasi platform Barracuda, integrasi Azure AD, Exchange Online, dan SMTP routing.
5	Aktivasi Fitur Keamanan	3 hari kerja	Aktivasi dan fine-tuning seluruh modul: Anti-Spam, Anti-Phishing, Sandboxing, DLP, Encryption, dll.
6	Policy Configuration	3 hari kerja	Konfigurasi kebijakan keamanan email, whitelist/blacklist, DLP policy, dan enkripsi.
7	Testing & UAT	3 hari kerja	User Acceptance Testing, pengujian skenario ancaman, dan validasi mail flow normal.
8	Dokumentasi	2 hari kerja	Finalisasi as-built document, SOP, dan seluruh dokumen deliverable.
9	Transfer Knowledge & Pelatihan	2 hari kerja	Pelaksanaan sesi pelatihan untuk tim TI internal.
10	Go-Live & Serah Terima	1 hari kerja	Serah terima dokumen, BAST, dan pernyataan selesai pekerjaan.
11	Dukungan Teknis Ongoing	12 bulan	Layanan support, preventive maintenance, dan quarterly report selama masa kontrak.

Total durasi implementasi awal: ±31 hari kerja sejak penandatanganan kontrak. Layanan dukungan teknis dan maintenance berlangsung selama 12 (dua belas) bulan terhitung sejak tanggal go-live.

## VII KRITERIA DAN KUALIFIKASI VENDOR

### 7.1 Kualifikasi Teknis

- Merupakan Partner Resmi Barracuda Networks (Barracuda Authorized Partner) yang dapat diverifikasi pada portal resmi Barracuda Networks. **(Optional)**
- Diutamakan memiliki status Barracuda Gold Partner, Platinum Partner, atau setara (dibuktikan dengan sertifikat resmi). **(Optional)**
- Memiliki tenaga teknis bersertifikat resmi Barracuda (Barracuda Certified Engineer atau setara). **(Optional)**
- Memiliki engineer yang memiliki pengetahuan mendalam tentang Microsoft 365, Exchange Online, Azure Active Directory, dan SMTP routing. **(Optional)**
- Memiliki pengalaman implementasi Barracuda Email Security **(Optional)**
- Memiliki infrastruktur helpdesk dan sistem manajemen tiket yang dikelola dengan baik (Whatsapp Group).

### 7.2 Dokumen yang Harus Dilampirkan

- Sertifikat Authorized Partner Barracuda Networks yang masih valid. **(Optional)**
- Sertifikat teknis tenaga ahli yang ditugaskan (Barracuda Certified Engineer atau setara). **(Optional)**
- Referensi proyek sejenis di email security **(Optional)**
- Profil perusahaan (Company Profile) dan portofolio proyek keamanan siber.
- Curriculum Vitae (CV) tenaga ahli yang akan ditugaskan. **(Optional)**

## VIII SERVICE LEVEL AGREEMENT (SLA)

### 8.1. Klasifikasi Tingkat Insiden

Prioritas	Definisi Insiden	Target Respons	Target Resolusi
Critical (P1)	Platform Barracuda tidak dapat diakses; seluruh email tidak dapat difilter; infeksi malware masif melalui email; ancaman aktif yang menyebar.	≤ 30 Menit	≤ 4 jam
High (P2)	Fitur kritis tidak berfungsi (Anti-Phishing, Anti-Malware down); false negative masif; lebih dari 20% pengguna tidak terlindungi; DLP tidak berjalan.	≤ 30 Menit	≤ 8 jam
Medium (P3)	False positive berulang yang mengganggu operasional; fitur non-kritis tidak berfungsi; isu performa dashboard;	≤ 30 Menit	≤ 15 jam

Prioritas	Definisi Insiden	Target Respons	Target Resolusi
	quarantine tidak dapat diakses sebagian pengguna.		
Low (P4)	Pertanyaan teknis; permintaan perubahan konfigurasi minor; konsultasi umum; request whitelist / blacklist.	≤ 30 Menit	≤ 1 hari kerja

## 8.2. Jam Layanan

- Layanan dukungan untuk insiden kategori P1 (Critical) dan P2 (High) tersedia 24x7 (setiap hari dan setiap waktu), termasuk di luar jam kerja, hari libur nasional, dan akhir pekan.
- Layanan dukungan untuk insiden kategori P3 (Medium) dan P4 (Low) tersedia pada jam kerja (Business Hours), yaitu Senin–Jumat pukul 09.00–18.00 WIB.
- Support: live chat (whatsapp), dan remote assistance (TeamViewer, AnyDesk, atau lainnya).
- Eskalasi ke Barracuda Networks Support Center untuk isu teknis yang memerlukan penanganan dari principal.

## IX KELUARAN

Penyedia jasa wajib menghasilkan dan menyerahkan seluruh keluaran berikut kepada pemberi kerja:

### 9.1 Dokumen Teknis

- Dokumen Hasil Assessment Awal: Inventarisasi mailbox aktif, konfigurasi DNS (MX, SPF, DKIM, DMARC), topologi mail flow Microsoft 365, dan kondisi keamanan email eksisting.
- Solution Design Document (HLD & LLD): Arsitektur solusi Email Security Barracuda, detail teknis konfigurasi, parameter integrasi dengan Microsoft 365 / Exchange Online, dan rencana deployment.
- As-Built Configuration Document: Dokumentasi seluruh konfigurasi final yang telah diterapkan pada platform Barracuda di lingkungan produksi, termasuk policy, rule, dan connector.
- Materi Transfer Knowledge: Slide pelatihan administrasi dan operasional, panduan pengguna (user guide) dalam Bahasa Indonesia, dan video tutorial (jika tersedia).

### 9.2 Deliverable Lisensi

- Sertifikat Lisensi Resmi **Barracuda Email Security ADVANCED for Microsoft 365** untuk seluruh mailbox terdaftar.
- Bukti aktivasi lisensi yang dapat diverifikasi melalui portal resmi Barracuda Networks.
- Jadwal perpanjangan lisensi beserta mekanisme notifikasi otomatis minimal 60 hari sebelum tanggal kadaluarsa.

### 9.3 Laporan Berkala

- Laporan Preventive Maintenance: Laporan per 3 bulan mencakup seluruh item pemeriksaan kesehatan platform, status update engine/signature, review policy, dan temuan selama periode berjalan.

- Laporan Corrective Maintenance: Laporan penanganan insiden per kejadian beserta analisis akar masalah (root cause analysis) dan rekomendasi pencegahan.
- Quarterly Report: Laporan komprehensif postur keamanan email setiap 3 (tiga) bulan, mencakup statistik ancaman, efektivitas filtering, dan evaluasi pencapaian SLA.
- Laporan Akhir Kontrak: Ringkasan seluruh layanan yang telah diberikan, rekapitulasi pencapaian SLA, statistik insiden, dan rekomendasi untuk periode kontrak berikutnya.

#### 9.4 Bukti Kehadiran dan Aktivitas

- Berita Acara Serah Terima (BAST) untuk setiap milestone pekerjaan yang telah diselesaikan.
- Daftar hadir peserta dan materi pelatihan transfer knowledge yang ditandatangani oleh peserta.
- Log tiket dukungan teknis (support ticket log) selama masa kontrak beserta status penyelesaian masing-masing tiket.
- Bukti pelaksanaan housekeeping maintenance per kuartal yang terdokumentasi dan ditandatangani oleh penanggung jawab teknis kedua belah pihak.

## X Timelin Proses Pengadaan

		Tanggal Mulai (Sejak Perencanaan)		5/13/2026
		Tanggal Mulai Pengadaan		5/18/2026
Tahap	Durasi (Hari)	Kegiatan Operasional	Unsur Bertanggung Jawab	Jadwal
Pelaksanaan & Evaluasi	2	Pendaftaran	Unsur Pengadaan	5/20/2026
	1	Evaluasi Peserta	Unsur Pengadaan	5/21/2026
	1	Penjelasan Dokumen (Aanwijzing)	User & Pengadaan	5/22/2026
	4	Batas Waktu Pemasukan Penawaran	Penyedia	5/26/2026
	1	Evaluasi Administratif & Penawaran	Tim Pengadaan/Unit Pengadaan	5/27/2026
	7	Negosiasi & Klarifikasi	Tim Pengadaan/Unit Pengadaan	6/3/2026
Penetapan & Perikatan	2	Penetapan Pemenang	Tim Pengadaan/Unit Pengadaan	6/5/2026
	3	Pengumuman Pemenang Sementara	Unsur Pengadaan	6/8/2026
	4	Masa Sanggahan	Penyedia	6/12/2026
	1	SIK (Surat Instruksi Kerja)	Tim Pengadaan/Unit Pengadaan	6/13/2026
	11	Otorisasi & Kontrak	Pejabat Berwenang & Unsur Legal	6/24/2026

- Note:**
- Jadwal diatas tidak termasuk hari libur (hanya hari kerja)
  - Komposisi Penilaian Evaluasi Seleksi adalah **70 % Teknis**, dan **30% Harga**.

## XI Harga Perkiraan Sendiri (HPS)

Produk	Kuantitas	Satuan	HPS (Rp)/tahun
<ul style="list-style-type: none"><li><i>Lisensi Barracuda Email Security type Advanced</i></li><li><i>Managed Support : Preventive Maintenance, Corrective Maintenance</i></li></ul>	100	Paket (bundle)	200.000.000

## XII PENUTUP

Dokumen ini menjadi acuan pelaksanaan pengadaan Perangkat Email Security untuk mendukung kestabilan operasional perangkat jaringan dan memastikan keberlangsungan layanan TI.

Hormat Kami,  
**Divisi Teknologi Informasi**

Menyetujui,



**Oki Marsetiawan**  
Kepala Divisi Teknologi  
Informasi

Pembuat Dokumen,



**Krisna Aji Putra**  
Staf Divisi Teknologi  
Informasi