Số và ký hiệu: 442/NB-KT
Ngày ban hành: 16/11/2026

THƯ MỜI QUAN TÂM

(Kèm theo Công văn số /KT-NB ngày tháng năm 2026)

I. Mô tả nhu cầu:

Tổng công ty Điện lực Dầu khí Việt Nam – CTCP (PV Power) có nhu cầu về việc thuê dịch vụ kiểm tra đánh giá, đảm bảo ATTT và hỗ trợ ứng cứu sự cố an ninh mạng.

II. Phạm vi công việc và yêu cầu:

1. Phạm vi công việc:

STT	Hạng mục công việc	Đơn vị tính	Số lượng	Thời gian triển khai
I	**Thuê dịch vụ kiểm tra đánh giá, đảm bảo ATTT và hỗ trợ ứng cứu sự cố an ninh mạng.**	**Gói**	**01**	**01 năm**
1	Đánh giá điểm yếu, kiểm thử xâm nhập (Pentest) ứng dụng nội bộ.			
2	Săn tìm mối nguy hại (Threat Hunting) trên hệ thống máy chủ.			
3	Rà soát, kiểm tra tính phù hợp và hiệu chỉnh hồ sơ đề xuất cấp độ 2 và các quy định bảo đảm ATTT của Cơ quan Tổng công ty.			
4	Xây dựng bổ sung các quy trình, quy định an toàn thông tin của Tổng công ty Điện lực Dầu khí Việt Nam – CTCP.			

Số và ký hiệu: 442/NB-KT
Ngày ban hành: 16/11/2026

2. Yêu cầu kỹ thuật cụ thể:

STT	Hạng mục công việc	Yêu cầu kỹ thuật
A	**KIỂM TRA, ĐÁNH GIÁ KỸ THUẬT (RÀ QUÉT LỖ HỔNG, PENTEST, SĂN TÌM MỐI NGUY HẠI)**	
1	**Đánh giá điểm yếu, kiểm thử xâm nhập (Pentest) ứng dụng nội bộ.**	**1.1. Phạm vi, đối tượng và tần suất** - **Đối tượng:** 07 ứng dụng nội bộ tại Cơ quan Tổng công ty và Trung tâm dữ liệu Viettel IDC, gồm: Email, VOffice, HiStaff, CMMS, KMS, SAP, Power Monitoring. - **Tần suất:** 01 lần/năm. **1.2. Nội dung và yêu cầu** - Rà quét, phân tích điểm yếu và kiểm thử xâm nhập có kiểm soát đối với từng ứng dụng nhằm xác định khả năng bị khai thác thực tế; đề xuất biện pháp khắc phục chi tiết cho từng lỗ hổng, gồm hướng dẫn kỹ thuật, phương án giảm thiểu tạm thời (nếu chưa thể vá ngay) và kiến nghị cải tiến quy trình đối với lỗi logic nghiệp vụ. - **Tiêu chuẩn áp dụng** (một hoặc kết hợp, tùy loại ứng dụng): +Web App: OWASP Web Security Testing Guide (WSTG) v4.2, OWASP Top 10, PTES, NIST SP 800-115; +Desktop App: OWASP Desktop App Security Top 10; +Mobile App: OWASP Mobile Top 10, OWASP Mobile Application Security Testing Guide (MASTG); +Tổng quát: PTES, OSSTMM v3.0 – làm cơ sở xác định cách tiếp cận theo từng lớp và từng giai đoạn đánh giá. - **Phương pháp:** Graybox (hình thức hộp xám theo điểm b khoản 4 Điều 27 Nghị định số 331/2026/NĐ-CP). - **Cam kết:** không phá hoại hệ thống, không gây gián đoạn dịch vụ; thực hiện trong khung thời gian và môi trường được PV Power chấp thuận. Kế hoạch kiểm thử phải được PV Power phê duyệt về phạm vi, thời gian, phương pháp, đầu mối phối hợp và phương án xử lý dữ liệu thu được.

<table>
<tr><th>STT</th><th>Hạng mục công việc</th><th>Yêu cầu kỹ thuật</th></tr>
<tr><td></td><td></td><td>
1.3. Các bước thực hiện
<table>
<tr><th>Bước</th><th>Công việc</th><th>Nội dung thực hiện</th></tr>
<tr><td>1</td><td>Thu thập thông tin</td><td>- Khảo sát mục tiêu, thu thập thông tin ứng dụng: tên, phiên bản, nền tảng (Web/Desktop/Mobile/API), mô hình triển khai, endpoint và các dịch vụ liên quan.
- Tiếp nhận tài khoản kiểm thử theo từng vai trò (người dùng/quản trị) để đánh giá phân quyền và logic nghiệp vụ.
- Thống nhất phạm vi, giới hạn kiểm thử và khung thời gian thực hiện.</td></tr>
<tr><td>2</td><td>Rà quét lỗ hổng, điểm yếu</td><td>- Sử dụng công cụ tự động (Burp Suite, OWASP ZAP, Nuclei, Nikto…) rà soát điểm yếu kỹ thuật: lỗi cấu hình, injection, XSS, CSRF, lỗi xác thực…
- Tìm kiếm endpoint, thư mục ẩn, API và thông tin nhạy cảm bị lộ (enumeration); xác định các điểm đầu vào có khả năng bị khai thác.</td></tr>
<tr><td>3</td><td>Xác minh lỗ hổng, kiểm thử xâm nhập</td><td>- Kiểm thử có kiểm soát đối với các lỗ hổng có nguy cơ cao để xác minh khả năng khai thác.
- Sử dụng kỹ thuật phù hợp (payload thủ công, công cụ hỗ trợ, script tùy biến) để xây dựng PoC.
- Ghi nhận kết quả, hình ảnh minh chứng và mức độ ảnh hưởng thực tế.</td></tr>
<tr><td>4</td><td>Đánh giá mức độ nguy hiểm và báo cáo kết quả (lần 1)</td><td>- Phân loại lỗ hổng theo CVSS v3.1 hoặc tương đương: Nghiêm trọng/Cao/Trung bình/Thấp.
- Lập báo cáo cho từng ứng dụng, gồm: mô tả lỗ hổng và cách phát hiện; hình ảnh minh chứng; mức độ rủi ro; khuyến nghị khắc phục chi</td></tr>
</table>
</td></tr>
</table>

Số và ký hiệu: 442/NB-KT
Ngày ban hành: 16/11/2026

<table>
<tr><th>STT</th><th>Hạng mục công việc</th><th>Yêu cầu kỹ thuật</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td></td><td>tiết.</td></tr>
<tr><td>5–7</td><td>Khắc phục, tái đánh giá, báo cáo (lần 2)</td><td>- Áp dụng cho từng ứng dụng (tái kiểm thử các lỗ hổng đã phát hiện ở lần 1; báo cáo gồm danh sách lỗi đã khắc phục kèm minh chứng, lỗi mới phát sinh và kết luận mức độ an toàn hiện tại của ứng dụng).</td></tr>
</table>
1.4. Sản phẩm bàn giao
- Báo cáo kết quả kiểm thử xâm nhập (lần 1) và báo cáo kết quả tái đánh giá (lần 2) cho từng ứng dụng (07 ứng dụng).
</td></tr>
<tr><td>2</td><td>Săn tìm mối nguy hại (Threat Hunting) trên hệ thống máy chủ.</td><td>
2.1. Phạm vi, đối tượng và tần suất
- Đối tượng: máy chủ tại Cơ quan Tổng công ty, Trung tâm dữ liệu Viettel IDC, máy chủ do PV Power quản trị (website TCT) và máy tính quản trị hệ thống:
<table>
<tr><th>STT</th><th>Đối tượng</th><th>Số lượng</th><th>Ghi chú</th></tr>
<tr><td>1</td><td>Máy chủ, máy tính quản trị hệ thống</td><td>≤ 60</td><td>Bao gồm máy chủ vật lý (host) và máy chủ ảo (VM)</td></tr>
</table>
- Tần suất: định kỳ 01 lần/năm
2.2. Nội dung và yêu cầu
- Mục tiêu: phát hiện mã độc, dấu hiệu xâm phạm, lỗ hổng, điểm yếu và các mối đe dọa mà hệ thống giám sát tự động chưa phát hiện được; nhận biết sớm hoạt động đáng ngờ, chủ động phát hiện tấn công tiềm ẩn thay vì chỉ phản ứng khi sự cố đã xảy ra.
- Yêu cầu kỹ thuật: săn tìm nguy cơ chủ động bằng cách truy cập trực tiếp vào máy chủ/máy trạm, chạy công cụ đánh giá để xác định dấu hiệu bị tấn công và các mối đe dọa nâng cao; việc đánh giá dựa trên các giả thuyết xây dựng từ chiến thuật, kỹ thuật và quy trình (TTPs) đã biết theo MITRE ATT&CK, các nguồn Threat Intelligence và kinh nghiệm xử lý sự cố.
</td></tr>
</table>

<table>
<tr><th>STT</th><th>Hạng mục công việc</th><th>Yêu cầu kỹ thuật</th></tr>
<tr><td></td><td></td><td>
- Phạm vi loại trừ: không bao gồm điều tra chuyên sâu và xử lý sự cố; trường hợp phát hiện sự cố, nhà thầu thông báo ngay cho PV Power, cung cấp thông tin ban đầu và khuyến nghị xử lý..
2.3. Các bước thực hiện
<table>
<tr><th>Bước</th><th>Công việc</th><th>Nội dung thực hiện</th></tr>
<tr><td>1</td><td>Khảo sát hiện trạng</td><td>- Thu thập thông tin về môi trường và các hệ thống cần đánh giá: hệ điều hành và phiên bản, địa chỉ IP, hostname, các dịch vụ đang chạy, thư mục webroot.</td></tr>
<tr><td>2</td><td>Chuẩn bị công cụ</td><td>- Truy cập thử (onsite hoặc remote) vào các máy cần đánh giá để xác nhận đủ quyền thực hiện.
- Chạy thử công cụ trên từng loại hệ điều hành để đánh giá hiệu năng và độ tương thích.
- Gửi PV Power danh sách công cụ sử dụng (mô tả, nguồn tham chiếu).</td></tr>
<tr><td>3</td><td>Thực hiện đánh giá</td><td>- Kết nối với quyền Administrator/root qua RDP/SSH… vào các máy cần đánh giá.
- Sao chép và chạy công cụ đánh giá; trích xuất log về một máy tổng hợp để phân tích.
- Xóa công cụ đánh giá khỏi các máy sau khi hoàn thành.
- Hình thức thực hiện: Onsite (kết nối trực tiếp và thực hiện đánh giá) hoặc Remote (PV Power hỗ trợ kênh truy cập, xuất log).</td></tr>
<tr><td>4</td><td>Báo cáo kết quả</td><td>- Tổng hợp danh sách đối tượng, kỹ thuật đã săn tìm và kết quả tương ứng.
- Đối với mối nguy hại phát hiện được: nêu rõ mức độ nghiêm trọng,</td></tr>
</table>
</td></tr>
</table>

Ban Kỹ thuật - 14:57 16/11/2026 - Văn thư Ban Kỹ thuật - Ban KT - Nguyễn Xuân Thành - 14:32 16/11/2026 - da ký - Phó Trưởng Ban KT

Số và ký hiệu: 442/NB-KT
Ngày ban hành: 16/11/2026

STT	Hạng mục công việc	Yêu cầu kỹ thuật
		dấu hiệu bị tấn công/xâm phạm (thông tin sơ bộ, vị trí bị xâm phạm, đường dẫn mẫu mã độc, registry, process…), các chỉ số xâm phạm (IoC) hoặc chỉ số tấn công (IoA). - Khuyến nghị (không tác động trực tiếp vào hệ thống) về cách xác định, gỡ bỏ các dấu hiệu phát hiện được, phương án ngăn ngừa sự cố tương tự và cải thiện an ninh hệ thống. **2.4. Sản phẩm bàn giao** - Báo cáo kết quả đánh giá xâm nhập và săn tìm mối nguy hại (01 lần/năm).
B	**ĐÁNH GIÁ TUÂN THỦ TẠI ĐƠN VỊ**	
3	**Rà soát, kiểm tra tính phù hợp và hiệu chỉnh hồ sơ đề xuất cấp độ 2 và các quy định bảo đảm ATTT của Cơ quan Tổng công ty.**	**3.1. Phạm vi** - Hồ sơ đề xuất cấp độ 2 đối với Hệ thống thông tin nội bộ của Tổng công ty Điện lực Dầu khí Việt Nam – CTCP; - 03 quy định hiện hành: Quy định bảo đảm an toàn thông tin (Quyết định số 1116/QĐ-ĐLDK ngày 04/12/2024); Quy định quản lý hệ thống công nghệ thông tin (Quyết định số 575/QĐ-ĐLDK ngày 15/10/2018); Quy định bảo đảm an ninh, an toàn thông tin trên môi trường máy tính, mạng máy tính (Quyết định số 574/QĐ-ĐLDK ngày 15/10/2018). **3.2. Nội dung và yêu cầu** - Rà soát, cập nhật, hiệu chỉnh Hồ sơ đề xuất cấp độ 2 và tài liệu thuyết minh đề xuất cấp độ theo hiện trạng mới nhất, phù hợp với Nghị định số 331/2026/NĐ-CP ngày 19/8/2026 của Chính phủ: tiêu chí xác định cấp độ 2 (Điều 12), thẩm quyền và trình tự thẩm định, phê duyệt (Điều 18, Điều 20), thành phần hồ sơ đề xuất cấp độ (Điều 21) và thuyết minh hồ sơ (Điều 22). - Rà soát, cập nhật phương án bảo đảm an ninh mạng theo Điều 29 Nghị định số 331/2026/NĐ-CP, bảo

STT	Hạng mục công việc	Yêu cầu kỹ thuật
		đảm đáp ứng yêu cầu cấp độ 2 của TCVN 14423:2026 và xử lý các khoảng trống phát hiện được khi đối chiếu. - Kiểm tra tính phù hợp, rà soát, cập nhật, hiệu chỉnh 03 quy định nêu trên. - **Hợp nhất** kết quả rà soát thành **01 Quy định** thống nhất về bảo đảm An ninh mạng của Tổng công ty. Quy định hợp nhất là Quy định bảo đảm an ninh mạng của Tổng công ty Điện lực Dầu khí Việt Nam - CTCP, phải được cấp có thẩm quyền phê duyệt, ban hành.. Quy định hợp nhất phải bao gồm các nội dung: quản lý, vận hành hệ thống thông tin (quản trị hệ thống, máy chủ, mạng, ứng dụng, cơ sở dữ liệu, phân quyền); quản lý truy cập mạng từ xa (VPN, xác thực đa yếu tố, truy cập của quản trị viên/nhà cung cấp, ghi nhật ký); sử dụng Internet, email và thiết bị đầu cuối (email, USB, Internet, máy tính cá nhân, mật khẩu, phòng chống mã độc..). Ngoài ra, Quy định phải bao quát đầy đủ các tiêu chí về yêu cầu quản lý theo TCVN 14423:2026 đối với hệ thống thông tin cấp độ 1, 2, 3, 4 của Tổng công ty, trong đó phải đáp ứng đầy đủ yêu cầu quản lý cấp độ 2 đối với hệ thống thuộc phạm vi Hồ sơ đề xuất cấp độ. **3.3. Sản phẩm bàn giao** - Hồ sơ đề xuất cấp độ 2 và tài liệu thuyết minh đã được cập nhật, hiệu chỉnh; - Phương án bảo đảm an ninh mạng đã được cập nhật và dự thảo Quyết định phê duyệt phương án (theo Mẫu số 07 kèm Nghị định số 331/2026/NĐ-CP); - Dự thảo Quy định bảo đảm an ninh mạng của Tổng công ty Điện lực Dầu khí Việt Nam – CTCP (sau khi hợp nhất 03 quy định nêu trên); - Bảng đối chiếu, thuyết minh các nội dung sửa đổi, bổ sung so với các quy định hiện hành.
4	**Xây dựng bổ sung các quy trình, quy định an toàn thông tin của Tổng công ty Điện lực Dầu khí**	**4.1. Phạm vi** - Xây dựng 10 quy định, quy trình đảm bảo an ninh mạng nêu tại mục 4.2, **4.2. Nội dung và yêu cầu**

Số và ký hiệu: 442/NB-KT
Ngày ban hành: 16/11/2026

<table>
<tr><th>STT</th><th>Hạng mục công việc</th><th>Yêu cầu kỹ thuật</th></tr>
<tr><td></td><td>Việt Nam – CTCP.</td><td>
<table>
<tr><th>STT</th><th>Quy trình</th><th>Nội dung chính</th></tr>
<tr><td>1</td><td>Quy định Quản lý tài khoản và truy cập</td><td>Cấp mới, thay đổi, khóa/xóa tài khoản; phân quyền theo vai trò (RBAC); rà soát định kỳ; quản lý tài khoản đặc quyền</td></tr>
<tr><td>2</td><td>Quy trình Quản lý thay đổi (Change Management)</td><td>Phê duyệt, đánh giá tác động, sao lưu, triển khai, kiểm thử, hoàn tác (rollback)</td></tr>
<tr><td>3</td><td>Quy trình Quản lý lỗ hổng và bản vá</td><td>Rà quét lỗ hổng, đánh giá mức độ, cập nhật bản vá, xử lý ngoại lệ</td></tr>
<tr><td>4</td><td>Quy định Sao lưu và khôi phục dữ liệu</td><td>Lịch sao lưu, phạm vi, thời gian lưu giữ, kiểm tra khả năng khôi phục, bản sao dự phòng</td></tr>
<tr><td>5</td><td>Quy trình Ứng phó và xử lý sự cố ATTT</td><td>Phát hiện → phân loại → cô lập → xử lý → khôi phục → báo cáo → rút kinh nghiệm</td></tr>
<tr><td>6</td><td>Quy định Quản lý tài sản thông tin (phần mềm và thiết bị CNTT)</td><td>Cài đặt, cập nhật, kiểm soát phần mềm/thiết bị; danh mục phần mềm không được phép</td></tr>
<tr><td>7</td><td>Quy trình Quản lý nhà cung cấp/đơn vị bên ngoài</td><td>Cam kết bảo mật, tài khoản nhà thầu, truy cập từ xa, giám sát và thu hồi quyền</td></tr>
<tr><td>8</td><td>Quy trình Kiểm tra, đánh giá ATTT định kỳ</td><td>Kiểm tra cấu hình, tài khoản, lỗ hổng, nhật ký, sao lưu, mức độ tuân thủ</td></tr>
<tr><td>9</td><td>Quy định Quản lý hồ sơ, tài liệu ATTT</td><td>Hồ sơ cấp độ, sơ đồ mạng, cấu hình, nhật ký, biên bản kiểm tra, hồ sơ sự cố</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>STT</th><th>Hạng mục công việc</th><th>Yêu cầu kỹ thuật</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td></td><td></td></tr>
<tr><td>10</td><td>Quy định quản lý truy cập từ xa</td><td>Các điều khoản liên quan đến việc truy cập từ xa vào hệ thống</td></tr>
</table>
- Các quy trình phải phù hợp với Nghị định số 331/2026/NĐ-CP, đáp ứng yêu cầu quản lý cấp độ 2 của TCVN 14423:2026, thống nhất với Quy định hợp nhất tại mục 3.2 và phù hợp với mô hình tổ chức, hiện trạng hệ thống của Tổng công ty.
- Mỗi quy trình bao gồm: mục đích, phạm vi áp dụng, trách nhiệm các bên, lưu đồ, diễn giải các bước và biểu mẫu kèm theo.
4.3. Sản phẩm bàn giao
- Bộ dự thảo 10 quy định, quy trình kèm biểu mẫu (bản mềm có thể chỉnh sửa và bản in).</td></tr>
<tr><td>5</td><td>Trực sẵn sàng 24/7 phối hợp với đơn vị cung cấp dịch vụ SOC của PV Power hỗ trợ ứng cứu sự cố an toàn thông tin</td><td>5.1. Phạm vi
- Hỗ trợ PV Power ứng cứu sự cố ATTT 24/7 trong thời gian 01 năm, phối hợp với đơn vị cung cấp dịch vụ SOC của PV Power và Đội ứng cứu sự cố của PV Power.
5.2. Nội dung và yêu cầu
- Điều tra, hỗ trợ khắc phục và tư vấn: phối hợp với đơn vị cung cấp dịch vụ SOC của PV Power và Đội ứng cứu sự cố của PV Power điều tra nguyên nhân, xác định phạm vi và mức độ tác động của sự cố; đưa ra khuyến nghị xử lý; hỗ trợ và tư vấn cho PV Power trong suốt quá trình khắc phục sự cố.</td></tr>
<tr><td>C</td><td colspan="2">YÊU CẦU NĂNG LỰC NHÂN SỰ</td></tr>
<tr><td>1</td><td>Quản lý dự án: 01</td><td>Tối thiểu 03 năm kinh nghiệm trong lĩnh vực ATTT và giữ vai trò Quản lý dự án ít nhất 01 dự án/gói thầu về dịch vụ đánh giá an toàn thông tin; Có trình độ đại học trở lên về một trong các chuyên ngành thuộc lĩnh vực CNTT, An toàn thông tin, Toán Tin, Điện tử viễn thông; Có chứng chỉ về chuyên môn Quản lý dự án PMP (Project Management Professional); Có ít nhất 03 trong các chứng chỉ chuyên môn Kiểm tra, đánh giá an</td></tr>
</table>

STT	Hạng mục công việc	Yêu cầu kỹ thuật
		thông tin còn hiệu lực thuộc danh sách sau: OSEP (Offensive Security Experienced Pentester); OSWE (Offensive Security Web Expert); OSCP (Offensive Security Certified Professional).
2	**Trưởng nhóm dự án: 01**	Tối thiểu 10 năm kinh nghiệm trong lĩnh vực ATTT hoặc đã trực tiếp tham gia ít nhất 03 dự án/ hợp đồng về dịch vụ đánh giá an toàn thông tin, trong đó ít nhất 01 dự án/hợp đồng làm trưởng nhóm dự án; Có trình độ đại học trở lên về một trong các chuyên ngành thuộc lĩnh vực CNTT, An toàn thông tin, Toán Tin, Điện tử viễn thông; Có chứng chỉ chuyên môn về quản trị An toàn thông tin CISSP (Certified Information Systems Security Professional) còn hiệu lực; Có ít nhất 03 chứng chỉ chuyên môn Kiểm tra, đánh giá An thông tin còn hiệu lực thuộc danh sách sau: OSCE³ (OffSec Certified Expert³); OSCE (Offensive Security Certified Expert); OSCP (Offensive Security Certified Professional); Đã từng nghiên cứu và công bố các lỗ hổng an toàn thông tin với số lượng ít nhất 2 CVE (Từ năm 2020 trở lại đây) với số điểm CVSS 3.1 từ 8.5 trở lên của các hãng như Microsoft, Facebook, Zoho ManageEngine,…
3	**Chuyên gia triển khai: 05**	Tối thiểu 03 năm kinh nghiệm trong lĩnh vực ATTT hoặc các nhân sự đã tham gia triển khai ít nhất 03 dự án về an toàn thông tin; Có trình độ đại học trở lên về một trong các chuyên ngành thuộc lĩnh vực CNTT, An toàn thông tin, Toán Tin, Điện tử viễn thông; Có ít nhất 01 trong các chứng chỉ chuyên môn Kiểm tra, đánh giá an thông tin còn hiệu lực thuộc danh sách sau: OSEP (Offensive Security Experienced Pentester); OSWE (Offensive Security Web Expert); OSCP (Offensive Security Certified Professional); OSCE (Offensive Security Certified Expert); Yêu cầu 01 trong 05 nhân sự có tối thiểu 01 nhân sự có chứng chỉ OSCE³(OffSec Certified Expert³); 01 nhân sự có nghiên cứu và công bố các lỗ hổng an toàn thông tin với số lượng ít nhất 5 CVE (Từ năm 2020 trở lại đây) với số điểm CVSS3.1 từ 7.0 trở lên và tối thiểu 01 nhân sự có về quản trị An toàn thông tin CISSP (Certified Information Systems Security Professional) còn hiệu lực.

3. Yêu cầu đề xuất:

Đơn vị cung cấp dịch vụ cần có kinh nghiệm triển khai hợp đồng tương tự.

Số và ký hiệu: 442/NB-KT
Ngày ban hành: 16/11/2026

Nội dung đề xuất bao gồm:

- Giới thiệu năng lực, kinh nghiệm của đơn vị.
- Lý lịch chuyên gia thực hiện công việc.
- Báo giá đối với dịch vụ.

Kính mời các đơn vị cung cấp dịch vụ quan tâm gửi nội dung đề xuất đến địa chỉ: Ban Kỹ thuật, Tổng công ty Điện lực Dầu khí Việt Nam - CTCP, 199 Nguyễn Tuân, Thanh Xuân, Hà Nội và gửi bản mềm qua email: nguyenthicamtu@pvpower.vn trước 09h00 ngày 25/11/2026.

Văn thư Ban Kỹ thuật - Ban Kỹ thuật - 14:57 16/11/2026 - Văn thư Ban Kỹ thuật - Ban Kỹ thuật - 14:57 16/11/2026 - Văn thư Ban Kỹ thuật - Ban KT
Phó Trưởng Ban KT - Nguyễn Xuân Thành - 14:32 16/11/2026 - đa ky - Phó Trưởng Ban KT - Nguyễn Xuân Thành - 14:32 16/11/2026 - đa ky - Phó Trưởng Ban KT