PHỤ LỤC: MÔ TẢ CÔNG VIỆC, YÊU CẦU TUYỂN DỤNG CÁC VỊ TRÍ THEO ĐỊNH BIÊN LAO ĐỘNG NĂM 2026 TẠI TRUNG TÂM CNTT

STT	Tên vị trí tuyển dụng	Tên VTCD	Đơn vị tuyển dụng	Số lượng chỉ tiêu	Nguồn tuyển dụng	Mô tả công việc	Yêu cầu độ tuổi	Trình độ chuyên môn	Trình độ ngoại ngữ	Kinh nghiệm công tác
1	**Chuyên viên GRC**	**Chuyên viên GRC Cấp 2/3/4**	**Phòng An ninh bảo mật**	1	Ngoài hệ thống	**Quản lý chính sách bảo mật:** - Quản lý các chính sách, quy định, quy trình về an toàn bảo mật hệ thống thông tin. - Lập kế hoạch triển khai thực hiện tuân thủ theo các chính sách, quy định của Nhà nước và BIDV đối với lĩnh vực an toàn bảo mật CNTT. - Nghiên cứu và đề xuất xây dựng các chính sách, quy trình về an toàn bảo mật thông tin tuân thủ theo các quy định của pháp luật, và theo các tiêu chuẩn/thông lệ quốc tế. **Rà soát, quản lý lỗ hổng bảo mật:** - Thực hiện rà soát điểm yếu bảo mật, kiểm toán bảo mật các thành phần trong hệ thống CNTT (máy chủ, ứng dụng, cơ sở dữ liệu, thiết bị mạng, thiết bị bảo mật, …) để phát hiện các điểm yếu, rủi ro về an toàn bảo mật đang tồn tại. - Đánh giá mức độ ảnh hưởng của các điểm yếu bảo mật đối với hệ thống để đưa ra phương án và khuyến nghị khắc phục. - Cảnh báo, hướng dẫn và phối hợp với các bộ phận khác xử lý các điểm yếu bảo mật được cảnh báo. - Kiểm tra, rà soát kết quả khắc phục các điểm yếu bảo mật.	≤ 35 tuổi tại thời điểm dự tuyển	**1. Trình độ chuyên môn:** Tốt nghiệp Đại học trở lên, hệ chính quy (bao gồm Đại học văn bằng 2, không bao gồm hình thức học liên thông lên Đại học) tại các trường Đại học trong nước hoặc các trường Đại học nước ngoài/liên kết quốc tế được công nhận theo quy định hiện hành. **2. Ngành/Chuyên ngành đào tạo:** Ứng viên đáp ứng điều kiện thuộc một trong hai nhóm chuyên môn sau: - Nhóm ngành Công nghệ – An ninh – Kỹ thuật: An toàn thông tin, Công nghệ thông tin, Khoa học máy tính, Kỹ thuật phần mềm, Điện tử – Viễn thông, Hệ thống thông tin, Toán – Tin, An ninh mạng, hoặc các ngành kỹ thuật liên quan. - Trường hợp đặc biệt: Ứng viên không đáp ứng yêu cầu về bằng cấp nhưng có chứng chỉ quốc tế uy tín (SANS/GIAC, Offensive Security, ISC2, EC-Council, ISACA) hoặc thành tích nổi bật (CTF, Bug Bounty, CVE/Hall of Fame) vẫn được xem xét tuyển dụng.	- Ưu tiên ứng viên đạt một trong các chứng chỉ tiếng Anh sau: TOEIC ≥ 600 / TOEFL PBT ≥ 500 / TOEFL CBT ≥ 173 / TOEFL iBT ≥ 61 / IELTS ≥ 5.5 / Cambridge FCE (B2 CEFR) / Bậc 4/6 theo Khung năng lực ngoại ngữ Việt Nam. - Trường hợp được tuyển dụng, ứng viên có trách nhiệm hoàn thiện điều kiện tiếng Anh theo quy định hiện hành của BIDV trong thời hạn được yêu cầu.	**Quản lý chính sách bảo mật:** - Có kinh nghiệm ít nhất 02 năm trong công tác quản lý chính sách bảo mật hoặc lĩnh vực liên quan. - Có hiểu biết về các tiêu chuẩn về an toàn bảo mật hệ thống thông tin ví dụ như: ISO 27001, PCI DSS, CIS, NIST, … - Tổ chức rà soát, đánh giá việc áp dụng các biện pháp đảm bảo an toàn bảo mật hệ thống thông tin theo cấp độ. - Triển khai và duy trì áp dụng các tiêu chuẩn an toàn bảo mật gồm PCI DSS, SWIFT CSP… - Có hiểu biết về lĩnh vực kiểm toán CNTT hoặc ATTT - Có kiến thức cơ bản về quản trị hệ thống, quản trị mạng, an ninh mạng, lỗ hổng ATTT. - Ưu tiên ứng viên có các chứng chỉ bảo mật như CISA/CRISC…, có kinh nghiệm về kiểm toán CNTT, ATTT, quản trị các dự án CNTT, ATTT. **Rà soát, quản lý lỗ hổng bảo mật:** - Đã có kinh nghiệm trong công tác rà soát, quản lý lỗ hổng bảo mật. - Có hiểu biết về các lỗ hổng bảo mật ứng dụng (OWASP Top 10, CWE, CVE) - Có hiểu biết về các tiêu chuẩn bảo mật ví dụ như ISO 27001 (ISO 27005), PCI DSS, CIS, NIST. - Thực hiện công tác quản lý điểm yếu bảo mật trên các hệ thống thông tin. - Tổ chức rà soát, đánh giá việc áp dụng các biện pháp đảm bảo an toàn bảo mật hệ thống thông tin theo cấp độ. - Triển khai và duy trì áp dụng các tiêu chuẩn an toàn bảo mật gồm PCI DSS, SWIFT CSP… - Ưu tiên ứng viên có các chứng chỉ bảo mật như CEH/CHFI/SECURITY+/CRISC…
2	**Chuyên viên SOC**	**Chuyên viên SOC Cấp 3/4**	**Phòng An ninh bảo mật**	2	Ngoài hệ thống	**Giám sát an ninh mạng 24x7 (SOC Tier 1):** - Giám sát SIEM/NDR/EDR trên giao diện tập trung; phát hiện & cảnh báo bất thường theo thời gian thực. - Tiếp nhận, phân loại (triage), xử lý bước đầu, escalate đúng SLA; kích hoạt SOAR/runbook. - Tổng hợp chỉ số, log sự kiện; đề xuất tinh chỉnh use-case, rule, playbook. **Quản trị vận hành SOC (Blue Team):** - Quản trị & vận hành SIEM, SOAR, EDR/EPP, NDR; điều tra & xử lý sự cố mức trung bình/khá. - Tiếp nhận và xử lý các sự cố an ninh mạng (Incident Response). - Phân tích, đánh giá ảnh hưởng, mức độ nghiêm trọng của các sự cố an ninh mạng và đưa ra biện pháp xử lý, phản ứng với các sự cố an ninh mạng. - Phát triển/tối ưu use-case, rule, detection analytics. - Kiểm thử phòng thủ (purple exercises), đề xuất hardening & giảm bề mặt tấn công. - Triển khai các công cụ, giải pháp giám sát an ninh mạng. - Hoàn thiện các quy trình vận hành, giám sát, xử lý sự cố an ninh mạng. **Phân tích sự kiện bảo mật (Forensic Team):** - Điều tra số: disk/memory/network forensics, trích xuất & phân tích artefact/log đa nền tảng. - Phân tích mã độc, dịch ngược phần mềm (Malware analysis - static/dynamic), phác thảo kill-chain/timeline, chỉ ra IoC & khuyến nghị. - Hỗ trợ vụ việc mức nghiêm trọng/cao, viết báo cáo kỹ thuật & executive. - Chủ động rà quét, săn tìm các nguy cơ bảo mật (Threat Hunting, Threat Intelligence) - Nghiên cứu, áp dụng các công nghệ mới về an ninh bảo mật. - Phát triển, tối ưu hóa và thực hiện phân tích giải pháp phát hiện nguy cơ, tăng hiệu quả của việc giám sát an ninh mạng và xử lý sự cố. - Tiếp nhận và đưa ra các giải pháp xử lý các sự kiện bảo mật mức độ ảnh hưởng cao/nghiêm trọng.	≤ 35 tuổi tại thời điểm dự tuyển	**1. Trình độ chuyên môn:** Tốt nghiệp Đại học trở lên, hệ chính quy (bao gồm Đại học văn bằng 2, không bao gồm hình thức học liên thông lên Đại học) tại các trường Đại học trong nước hoặc các trường Đại học nước ngoài/liên kết quốc tế được công nhận theo quy định hiện hành. **2. Ngành/Chuyên ngành đào tạo:** Ứng viên đáp ứng điều kiện thuộc một trong hai nhóm chuyên môn sau: - Nhóm ngành Công nghệ – An ninh – Kỹ thuật: An toàn thông tin, Công nghệ thông tin, Khoa học máy tính, Kỹ thuật phần mềm, Điện tử – Viễn thông, Hệ thống thông tin, Toán – Tin, An ninh mạng, hoặc các ngành kỹ thuật liên quan. - Trường hợp đặc biệt: Ứng viên không đáp ứng yêu cầu về bằng cấp nhưng có chứng chỉ quốc tế uy tín (SANS/GIAC, Offensive Security, ISC2, EC-Council, ISACA) hoặc thành tích nổi bật (CTF, Bug Bounty, CVE/Hall of Fame) vẫn được xem xét tuyển dụng.	- Ưu tiên ứng viên đạt một trong các chứng chỉ tiếng Anh sau: TOEIC ≥ 600 / TOEFL PBT ≥ 500 / TOEFL CBT ≥ 173 / TOEFL iBT ≥ 61 / IELTS ≥ 5.5 / Cambridge FCE (B2 CEFR) / Bậc 4/6 theo Khung năng lực ngoại ngữ Việt Nam. - Trường hợp được tuyển dụng, ứng viên có trách nhiệm hoàn thiện điều kiện tiếng Anh theo quy định hiện hành của BIDV trong thời hạn được yêu cầu.	**Giám sát an ninh mạng 24x7 (SOC Tier 1):** - Đã có kinh nghiệm về SOC/giám sát ANM hoặc thực tập dự án tương đương; nắm căn bản TCP/IP, OS, log. - Biết sử dụng SIEM/SOAR/EDR; ưu tiên biết MITRE ATT&CK, quy trình IR cơ bản. - Ưu tiên CEH/Security+/CHFI; tiếng Anh kỹ thuật đáp ứng đọc tài liệu & ca trực. **Quản trị vận hành SOC (Blue Team):** - Tối thiểu 2 năm vận hành/điều tra sự cố an ninh mạng; hiểu sâu Windows/Linux/AD, networking, log. - Thành thạo kịch bản Incident Response, containment/eradication, viết script (Python/PowerShell) là lợi thế. - Ưu tiên CEH/CHFI/GCIH/GMON/GCDA, có trải nghiệm CTF/Red vs Blue. **Phân tích sự kiện bảo mật (Forensic Team):** - Tối thiểu 2 năm DFIR/forensics/malware; thành thạo Volatility, YARA, Sysinternals, PCAP. - Biết reverse cơ bản (x86/x64), sandbox, memory dump; ưu tiên scripting (Python). - Ưu tiên CHFI/GCFA/GREM/GIAC IR; có CVE/white-paper là điểm cộng.
3	**Chuyên viên quản trị hệ thống (Hệ thống - Lưu trữ - Cloud)**	**Chuyên viên quản trị hạ tầng Cấp 3/4**	**Phòng Quản trị hạ tầng**	2	Ngoài hệ thống/ Nội bộ Khối CNTT	**1. Nhiệm vụ chung của Phòng Quản trị hạ tầng:** - Quản trị, vận hành toàn bộ hạ tầng CNTT trọng yếu: máy chủ, lưu trữ, mạng, cloud, sao lưu & dự phòng dữ liệu, đảm bảo ổn định – an toàn – sẵn sàng 24/7. - Triển khai, tối ưu, tự động hóa hạ tầng CNTT; đảm bảo khả năng mở rộng, dự phòng và hiệu năng hệ thống cho toàn ngân hàng. - Tham gia nghiên cứu, tích hợp công nghệ mới (Cloud, Container, Automation, AIOps) trong chiến lược chuyển đổi số BIDV. - Triển khai các dự án hạ tầng, giải pháp CNTT của BIDV. **2. Nhiệm vụ riêng các Nhóm (ứng viên sẽ được phân vào 1 trong 3 nhóm theo mức độ phù hợp)** **2.1. Nhóm Quản trị hệ thống:** - Quản trị các hệ thống máy chủ thường và các hệ thống máy chủ chuyên dụng của BIDV - Quản trị các hệ thống Active Directory, email, hệ điều hành Windows/Linux/Unix, nền tảng ảo hóa (VMware, Proxmox VE, PowerVM,...) của BIDV - Tham gia triển khai, bảo trì và tối ưu các hạ tầng máy chủ, hệ điều hành, dịch vụ nền tảng. - Tham gia nghiên cứu, thử nghiệm, triển khai các công cụ quản trị, các giải pháp, công nghệ mới về hệ thống (máy chủ, lưu trữ, sao lưu/phục hồi dữ liệu, ảo hóa...). **2.2. Nhóm Lưu trữ và bảo vệ dữ liệu:** - Quản trị hệ thống SAN/NAS/Object Storage, sao lưu – phục hồi dữ liệu bằng CommVault, Veeam, Veritas. - Đảm bảo an toàn, toàn vẹn, khả năng phục hồi dữ liệu cho các hệ thống trọng yếu (Core, Data Warehouse, Cloud). - Thực hiện giám sát, tối ưu, và diễn tập DR, triển khai giải pháp bảo vệ dữ liệu đa tầng. **2.3 Nhóm Quản trị hạ tầng Cloud** - Quản trị các hệ thống Private Cloud VCF, public Cloud (Quốc tế:Google Cloud, AWS và trong nước). - Triển khai và quản trị các nền tảng Container: K8S, VMWare Tanzu, OpenShift. - triển khai các công cụ giám sát, thu thập log, backup, tự động hóa công việc quản trị, IaaC (infrastructure as code) cho các hạ tầng Private Cloud, Public Cloud	≤ 35 tuổi tại thời điểm dự tuyển **(Không giới hạn tuổi đối với tuyển dụng nội bộ Khối CNTT)**	**1. Trình độ chuyên môn:** Tốt nghiệp Đại học trở lên, hệ chính quy (bao gồm Đại học văn bằng 2, không bao gồm hình thức học liên thông lên Đại học) tại các trường Đại học trong nước hoặc các trường Đại học nước ngoài/liên kết quốc tế được công nhận theo quy định hiện hành. **2. Ngành/Chuyên ngành đào tạo:** Ứng viên đáp ứng điều kiện thuộc một trong các ngành/chuyên ngành Công nghệ – Hạ tầng – Kỹ thuật: Công nghệ thông tin, An toàn thông tin, Khoa học máy tính, Hệ thống thông tin, Điện tử – Viễn thông, Toán – Tin, Kỹ thuật máy tính, hoặc các ngành kỹ thuật – công nghệ liên quan khác.	- Ưu tiên ứng viên đạt một trong các chứng chỉ tiếng Anh sau: TOEIC ≥ 600 / TOEFL PBT ≥ 500 / TOEFL CBT ≥ 173 / TOEFL iBT ≥ 61 / IELTS ≥ 5.5 / Cambridge FCE (B2 CEFR) / Bậc 4/6 theo Khung năng lực ngoại ngữ Việt Nam. - Trường hợp được tuyển dụng, ứng viên có trách nhiệm hoàn thiện điều kiện tiếng Anh theo quy định hiện hành của BIDV trong thời hạn được yêu cầu..	**Ứng viên đáp ứng 1 trong các nhóm kinh nghiệm sau:** **1. Quản trị Hệ thống (Servers / OS / AD / Email)** - Tối thiểu 02 năm kinh nghiệm quản trị hệ thống máy chủ và một trong các mảng công việc: Active Directory, DNS, Email, Windows/Linux/Unix Server, ảo hóa VMware/Proxmox VE/PowerVM. - Có hiểu biết về HA/DR, Backup/Restore, Clustering, Performance tuning; kỹ năng viết tài liệu & tư duy xử lý sự cố tốt. - Có kinh nghiệm quản trị và làm việc với nền tảng Redhat Openshift hoặc các hệ thống máy chủ AI là một lợi thế - Ưu tiên ứng viên có các chứng chỉ CKA, MCSA/MCSE, RHCSA/RHCE, VMware VCP, LPIC-2; - Hiểu quy trình vận hành Data Center là lợi thế. **2. Quản trị Lưu trữ & Sao lưu (Storage & Backup)** - Tối thiểu 02 năm kinh nghiệm quản trị hệ thống SAN/NAS/Object Storage, Backup/Recovery, hoặc DR site. - Am hiểu công nghệ lưu trữ RAID, iSCSI, FC, tiering, replication; thành thạo CommVault, Veeam, Veritas là lợi thế. - Ưu tiên chứng chỉ Dell EMC Storage Specialist, NetApp NCDA, Veeam VMCE, SNIA, hoặc có kinh nghiệm bảo vệ dữ liệu đa tầng. **3. Quản trị Cloud** Đối với ứng viên bên ngoài BIDV: • Có kinh nghiệm ít nhất 02 năm triển khai, quản trị hạ tầng Cloud của một trong các nhà cung cấp dịch vụ Cloud AWS, Google, Oracle • Có hiểu biết, kinh nghiệm về một trong các ảo hóa VMWare, Nutanix, Openshift. • Có hiểu biết, kinh nghiệm về một trong các nền tảng Container Openshift, Tanzu • Ưu tiên ứng viên có chứng chỉ Linux Professional Institute LPIC-2, AWS Certificate Solutions Architect Professional, Google Professional Cloud Architect Đối với ứng viên nội bộ: • Có tối thiểu 03 năm là chuyên viên công tác tại một trong các bộ phận quản trị hệ thống máy chủ, hệ thống lưu trữ tại các Ban/Trung tâm TSC. • Có tối thiểu 03 năm công tác tại BIDV, không trong thời gian bị xem xét thi hành kỷ luật hoặc đang trong thời gian thi hành kỷ luật.
4	**Chuyên viên bảo mật hạ tầng**	**Chuyên viên bảo mật hạ tầng Cấp 3/4**	**Phòng An ninh bảo mật**	2	Ngoài hệ thống	- Quản trị, vận hành và tối ưu hóa (hardening) các hệ thống bảo mật hạ tầng, bao gồm các hệ thống bảo mật mạng, bảo mật máy tính (Firewall, IPS, VPN, ZTNA, Microsegmentation, NAC, DNS Security, MDM, EDR/EPP, DLP...). - Xây dựng, đề xuất các yêu cầu về an toàn bảo mật đối với hệ thống bảo mật mạng, bảo mật máy tính. - Đầu mối đánh giá rủi ro, đề xuất các giải pháp, biện pháp an toàn bảo mật mạng, bảo mật máy tính cụ thể trên các môi trường on-premise hoặc cloud.	≤ 35 tuổi tại thời điểm dự tuyển	**1. Trình độ chuyên môn:** Tốt nghiệp Đại học trở lên, hệ chính quy (bao gồm Đại học văn bằng 2, không bao gồm hình thức học liên thông lên Đại học) tại các trường Đại học trong nước hoặc các trường Đại học nước ngoài/liên kết quốc tế được công nhận theo quy định hiện hành. **2. Ngành/Chuyên ngành đào tạo:** Ứng viên đáp ứng điều kiện thuộc một trong hai nhóm chuyên môn sau: - Nhóm ngành Công nghệ – An ninh – Kỹ thuật: An toàn thông tin, Công nghệ thông tin, Khoa học máy tính, Kỹ thuật phần mềm, Điện tử – Viễn thông, Hệ thống thông tin, Toán – Tin, An ninh mạng, hoặc các ngành kỹ thuật liên quan. - Trường hợp đặc biệt: Ứng viên không đáp ứng yêu cầu về bằng cấp nhưng có chứng chỉ quốc tế uy tín (SANS/GIAC, Offensive Security, ISC2, EC-Council, ISACA) hoặc thành tích nổi bật (CTF, Bug Bounty, CVE/Hall of Fame) vẫn được xem xét tuyển dụng.	- Ưu tiên ứng viên đạt một trong các chứng chỉ tiếng Anh sau: TOEIC ≥ 600 / TOEFL PBT ≥ 500 / TOEFL CBT ≥ 173 / TOEFL iBT ≥ 61 / IELTS ≥ 5.5 / Cambridge FCE (B2 CEFR) / Bậc 4/6 theo Khung năng lực ngoại ngữ Việt Nam. - Trường hợp được tuyển dụng, ứng viên có trách nhiệm hoàn thiện điều kiện tiếng Anh theo quy định hiện hành của BIDV trong thời hạn được yêu cầu.	- Tối thiểu 2 năm bảo mật mạng, bảo mật máy tính; am hiểu routing/switching, TLS, PKI, AD, OS hardening. - Có hiểu biết sâu về bảo mật mạng (Firewall, IPS và các giải pháp bảo mật mạng khác). - Có hiểu biết về các công nghệ nền tảng hạ tầng và cloud (on-prem and cloud infrastructure technologies). - Có hiểu biết sâu về các hệ điều hành máy tính Windows, Linux, Unix. - Có kinh nghiệm về các công nghệ và các giải pháp bảo mật cho máy trạm. - Ưu tiên ứng viên đã có kinh nghiệm trong công tác quản trị, vận hành các hệ thống bảo mật máy tính như Trellix, TrendMicro, Forescout, có các chứng chỉ bảo mật liên quan như Network+/CCNA Security, CySA+, Azure/AWS Security.
5	**Chuyên viên quản trị Cơ sở dữ liệu**	**Chuyên viên quản trị Cơ sở dữ liệu Cấp 3**	**Phòng Quản trị hạ tầng**	2	Ngoài hệ thống/ Nội bộ Khối CNTT	**1. Quản trị CSDL:** -Quản trị các hệ thống CSDL và các hệ thống CNTT đặc thù khác của CSDL tại BIDV ở mức độ quan trọng trung bình theo sự phân công của trưởng nhóm và Lãnh đạo phòng Quản trị Hạ tầng -Xây dựng, triển khai các hệ thống CSDL có mức độ quan trọng trung bình theo sự phân công của trưởng nhóm và Lãnh đạo phòng Quản trị Hạ tầng - Xử lý các vấn đề/sự cố có độ phức tạp trung bình, thực hiện hỗ trợ kỹ thuật thuộc mảng công việc được phân công quản trị - Giám sát, theo dõi cảnh báo các vấn đề liên quan CSDL -Tối ưu hệ thống định kỳ hoặc đột xuất các hệ thống CSDL: Phân tích xử lý ở mức độ trung bình, sử dụng thành thạo công cụ có sẵn và thực hiện theo hướng dẫn. Cập nhật bản vá và nâng cấp các hệ thống CSDL theo hướng dẫn. - Vận hành, duy trì hoạt động CSDL - Tiếp nhận/xử lý thông tin về các sự kiện Co sở dữ liệu - Tham gia xây dựng và góp ý, triển khai với quy trình/quy định trong mảng công việc được phân công quản trị và các mảng công việc liên quan -Tham gia nghiên cứu, nắm bắt công nghệ mới, đề xuất và Thực hiện các đề tài nghiên cứu về CSDL để áp dụng các công nghệ phù hợp vào hệ thống CNTT BIDV -Trực tiếp thực hiện công tác quản lý báo mật và phân quyền CSDL theo tài liệu. công tác quản trị, giám sát **2.Triển khai dự án/PAMS/Báo trì:** - Theo dõi và phối hợp thực hiện phương án bảo trì CSDL, các thiết bị CNTT -Tham gia triển khai các dự án, kế hoạch mua sắm liên quan đến CSDL và các dự án có liên quan của BIDV **3. Diễn tập** - Tham gia diễn tập dự phòng HA, DR, ứng cứu sự cố cho CSDL - Phối hợp xây dựng kịch bản và tổ chức diễn tập dự phòng HA, DR theo kịch bản. **4. Thực hiện các công tác khác** -Thực hiện một số nội dung thuộc nghiệp vụ Cơ sở dữ liệu do lãnh đạo phân công. -Tham gia các tổ/nhóm trong và ngoài Trung tâm CNTT	≤ 35 tuổi tại thời điểm dự tuyển **(Không giới hạn tuổi đối với tuyển dụng nội bộ Khối CNTT)**	**1. Trình độ chuyên môn:** Tốt nghiệp Đại học trở lên, hệ chính quy (bao gồm Đại học văn bằng 2, không bao gồm hình thức học liên thông lên Đại học) tại các trường Đại học trong nước hoặc các trường Đại học nước ngoài/liên kết quốc tế được công nhận theo quy định hiện hành. **2. Ngành/Chuyên ngành đào tạo:** Ứng viên đáp ứng điều kiện thuộc một trong các ngành/chuyên ngành/nhóm ngành Công nghệ – Dữ liệu – Kỹ thuật: Công nghệ thông tin, Khoa học máy tính, Hệ thống thông tin, Toán – Tin, An toàn thông tin, Kỹ thuật phần mềm, Điện tử – Viễn thông hoặc các ngành kỹ thuật – công nghệ khác có đào tạo về cơ sở dữ liệu và hệ thống thông tin.	- Ưu tiên ứng viên đạt một trong các chứng chỉ tiếng Anh sau: TOEIC ≥ 600 / TOEFL PBT ≥ 500 / TOEFL CBT ≥ 173 / TOEFL iBT ≥ 61 / IELTS ≥ 5.5 / Cambridge FCE (B2 CEFR) / Bậc 4/6 theo Khung năng lực ngoại ngữ Việt Nam. - Trường hợp được tuyển dụng, ứng viên có trách nhiệm hoàn thiện điều kiện tiếng Anh theo quy định hiện hành của BIDV trong thời hạn được yêu cầu..	**1. Kinh nghiệm:** **1.1. Đối với ứng viên ngoài BIDV:** - Tối thiểu 02 năm quản trị CSDL (triển khai, vận hành, tối ưu, sao lưu/khôi phục). - Ưu tiên: từng làm với HA/DR/Cluster, phân tích hiệu năng, xử lý sự cố phức tạp; có kinh nghiệm viết tài liệu & thuyết trình. - Chứng chỉ (khuyến khích): Oracle (OCA/OCP), PostgreSQL, SQL Server (MCSA/DP-300), Linux/Cloud cơ bản. **1.2. Đối với ứng viên nội bộ BIDV** - Ưu tiên cán bộ đang làm hạ tầng/ứng dụng có mình chứng tham gia quản trị/vận hành CSDL ≥ 01 năm. - Có đánh giá tốt về kỹ luật vận hành, phối hợp khối nghiệp vụ, tinh thần cải tiến/tự động hóa. - Cam kết hoàn thành chứng chỉ CSDL phù hợp trong thời hạn do đơn vị quy định. **2. Năng lực chuyên môn** - Nắm vững SQL, thiết kế lược đồ, phân quyền/kiểm soát truy cập, backup/restore, monitor & tuning. - Biết vận hành ít nhất 01 hệ CSDL: Oracle/SQL Server/PostgreSQL; hiểu NoSQL là lợi thế. - Kiến thức nền Hệ điều hành (Linux/Windows), mạng, lưu trữ, công cụ giám sát (OEM, Grafana/Prometheus, Zabbix…). **3. Năng lực mềm** - Phân tích & giải quyết vấn đề, giao tiếp phối hợp đội liên chức năng; cẩn trọng, tuân thủ quy trình thay đổi. - Chịu áp lực ca/kíp khi xử lý sự cố; tinh thần trách nhiệm – trung thực – chủ động học hỏi.
Tổng:				9						