

PHỤ LỤC: MÔ TẢ CÔNG VIỆC, YÊU CẦU TUYỂN DỤNG CÁC VỊ TRI ĐỢT 03 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 bảo mật hạ tầng	Chuyên viên bảo mật hạ tầng Cấp 3/4	Phòng an ninh bảo mật	2	Ngồi ở thông	- 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, SIEM Security, MDM, EDR/EP, DLP...).	≤ 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/nhiệt 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 và 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.	Tốt nhất 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 như Windows, Linux, Unix. - Có kinh nghiệm về các công nghệ và các giải pháp bảo mật cho máy trạm. - Ưu tiên ứng viên có các kinh nghiệm trong công tác quản trị, vận hành các hệ thống bảo mật máy tính như TrendMicro, Fortinet, hoặc các chứng chỉ bảo mật liên quan như Network/CCNA Security, CySA+, Azure/AWS Security.
2	Chuyên viên SOC	Chuyên viên SOC Cấp 3/4	Phòng an ninh bảo mật	1	Ngồi ở thông	Giám sát an ninh mạng 24/7 (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 hoặc đầu, escalate dùng SLA; kích hoạt SOAR/runbook. - Tổng hợp chỉ số, log và cảnh; để xuất tình hình use-case, rule, playbook. Quản trị vận hành SOC (Blue Team): - Quản trị & vận hành SIEM, SOAR, EDR/EP, NDR; điều tra & xử lý sự cố mức trung bình/nhẹ. - Tiếp nhận và xử lý sự cố 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/hiệu chỉnh use-case, rule, detection analytics. - Kiểm thử phòng thủ (purple exercises), để xuất hardening & giám bị mật tấn công. - Triển khai các công cụ, giải pháp giám sát an ninh mạng. - Nghiên cứu các quy trình vận hành, giám sát, xử lý sự cố an ninh mạng. Phân tích sự kiện bảo mật (Forensic Team): - Điều tra sự cố: disk/memory/network forensics, trích xuất & phân tích artefact/log đa nền tảng. - Phân tích mã độc, đặc ngược phần mềm (Malware analysis - static/dynamic), phân tích chuỗi thời gian (chain-of-custody), chỉ ra IOC & khuyến nghị. - Hỗ trợ vụ việc mức nghiêm trọng/cao, viết báo cáo kỹ thuật để executive. - Chịu đựng rủi ro quốc, dân tâm 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 sự cố kiến 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/nhiệt 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 và 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 24/7 (SOC Tier 1): - Đủ có kinh nghiệm về SOC/giám sát ANM hoặc thực tập dự án trong đường: nền 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 đạt ứng dụng tại địa & cụ 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 kiến thức Incident Response, containment/eradication, viết script (Python/PowerShell) là lợi thế. - Ưu tiên CEH/CHFI/CCRG/OS/OCDA, có tài năng/CTF/Red & Blue. Phân tích sự kiện bảo mật (Forensic Team): - Tối thiểu 2 năm DFR/forensics/malware; thành thạo Volatility, Yara, Sysinternals, PCAP. - Biết reverse cơ bản (x86/x64), sandbox, memory dump; ưu tiên scripting (Python). - Ưu tiên CHFI/OCFA/GREM/GIAC/IR; có CVE/write-paper là điểm cộng.
3	Chuyên viên GRC	Chuyên viên GRC Cấp 2/3/4	Phòng an ninh bảo mật	1	Ngồi ở thông	Quản lý chính sách bảo mật: - Quản lý các chính sách, quy định, quy trình về an toàn bảo mật hệ thống thông tin. - Xây kế hoạch triển khai thực hiện tuân thủ các tiêu chuẩn, quy định của Nhà nước và BIDV đối với lĩnh vực an toàn bảo mật CNTT. - Nghiên cứu và để xuất xây dựng các chính sách, quy trình về an toàn thông tin tuân thủ theo các quy định của pháp luật, và theo các tiêu chuẩn/hiệu lực quốc tế. Rà soát, quản lý hệ thống bảo mật: - Thực hiện rà soát định yếu bảo mật, kiểm toán bảo mật các thành phần trong hệ thống CNTT (mạng, 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. - Phân tích 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 các quy định khác 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/nhiệt 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 và 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 đa như: ISO 27001, PCI DSS, CIS, NIST, - Tài chính và soạn, đánh giá việc áp dụng các biện pháp đảm bảo an toàn bảo mật hệ thống thông tin theo cấp độ. - Trình bày 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 ATT. - Có kiến thức cơ bản về quản trị hệ thống, quản trị an ninh mạng, an ninh mạng, không ATT. - 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 hệ thống bảo mật: - Đủ có kinh nghiệm trong công tác rà soát, quản lý hệ thống bảo mật. - Có hiểu biết về các hệ thống bảo mật ứng dụng (OWASP Top 10, CWE, CVE). - Có hiểu biết về các tiêu chuẩn bảo mật và đa 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. - Tài chính và soạn, đánh giá việc áp dụng các biện pháp đảm bảo an toàn bảo mật hệ thống thông tin theo cấp độ. - Trình bày 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, ...
4	Chuyên viên quản trị Cơ sở dữ liệu	Chuyên viên quản trị Cơ sở dữ liệu Cấp 2/3	Phòng Quản trị hạ tầng	1	Ngồi ở thông/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 trong 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 trong 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. - Tham gia nghiên cứu, nắm bắt công nghệ mới, để xuất và Thực hiện các đề án nghiên cứu về CSDL, để áp dụng các công nghệ phù hợp vào hệ thống CNTT BIDV và nâng cấp các hệ thống CSDL, theo hướng dẫn. - Vận hành, duy trì hoạt động CSDL. - Tiếp nhận/ xử lý thông tin và các sự kiện Cơ sở dữ liệu. - Tham gia xây dựng và góp ý, triển khai với quy trình quy trình 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, để xuất và Thực hiện các đề án nghiên cứu về CSDL, để áp dụng các công nghệ phù hợp vào hệ thống CNTT BIDV. - Thực hiện một số nội dung thuộc nghiệp vụ Cơ sở dữ liệu do lãnh đạo phân công. 2. Triển khai dự án PAMS/Bảo 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. Điều tập: - Tham gia điều 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	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/nhiệt 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 và 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.	1. Kinh nghiệm: - Ưu tiên ứng viên có các chứng chỉ bảo mật như CEH/CHFI/SECURITY+ – CRISC, ... 1.1. Đối với ứng viên ngoài BIDV: - Tối thiểu 02 năm quản trị CSDL (triển khai, vận hành, tối ưu, sự cố, lưu trữ, khôi phục). - Ưu tiên: từng làm việc tại HADR/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 việc trong ứng dụng có minh chứng tham gia quản trị/vận hành CSDL ≥ 01 năm. - Có đánh giá tốt về kỹ thuật vận hành, phối hợp khối nghiệp vụ, tính toán chi tiêu tự động hóa. - Cam kết hoàn thiện chứng chỉ CSDL, phù hợp trong thời hạn do đơn vị quy định. 2. Năng lực chuyên môn - Nắm vững SQL, thiết kế lược & phân, quản lý/kiểm soát sự cố, backup/restore, monitor & tuning. - Biết vận hành & điều trị hệ CSDL: Oracle/SQL Server/PostgreSQL; hiểu NQL là lợi thế. - Kiến thức nền HADR (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 đối liên các chức năng; cần truen, tuân thủ quy trình thay đổi. - Chẩn áp lực cao/khí sự vụ cơ; tinh thần trách nhiệm – trung thực – chịu đựng khó khăn.
5	Chuyên viên Quản trị ứng dụng	Chuyên viên Quản trị ứng dụng khách hàng (02 chỉ tiêu) / Phòng Quản trị ứng dụng Nội bộ (03 chỉ tiêu)	Phòng Quản trị ứng dụng khách hàng (02 chỉ tiêu) / Phòng Quản trị ứng dụng Nội bộ (03 chỉ tiêu)	5	Ngồi ở thông/Nội bộ Khối CNTT	1. Quản trị và vận hành hệ thống: - Quản trị, vận hành, giám sát hoạt động của hệ thống phần mềm ứng dụng, nền tảng và lớp giữa đảm bảo ổn định, liên tục, an toàn. - Thực hiện kiểm soát tham số, quản lý tài khoản, nhất kỹ vận hành, đảm bảo tuân thủ các quy định an ninh, an toàn thông tin (ISO 27001). - Phối hợp xử lý sự cố, kiểm tra, nghiệm thu, báo tri, nâng cấp phần mềm, đảm bảo chất lượng và tiến độ theo quy định quản lý CNTT của BIDV. 2. Tổ chức, duy trì và đảm bảo tính sẵn sàng hệ thống - Rà soát, quy hoạch, tối ưu hiệu năng và dung lượng hệ thống để xuất, xây dựng phương án HA/DR, tổ chức diễn tập định kỳ. - Giám sát hoạt động hệ thống các công cụ chuyên dụng (Monitor tập trung, Application Manager, ELK, DataHub...), tổng hợp báo cáo SLA, chỉ số và tình trạng vận hành. - Đề xuất, thử nghiệm, triển khai nâng cấp phần mềm và hạ tầng kỹ thuật, đảm bảo khả năng mở rộng và các hệ thống quan trọng. 3. Phân tích, xử lý sự cố và đảm bảo an toàn vận hành - Phân tích, đánh giá, thử nghiệm nhận xét về (RCA) và khắc phục sự cố đối với các ứng dụng Banking, Thanh toán dịch vụ, Middleware và hệ thống hỗ trợ vận hành. - Rà soát bảo mật ứng dụng, tối ưu CSDL và hiệu năng, tổng hợp báo cáo định kỳ, để xuất biên bản phân tích theo cơ chế an toàn hệ thống. - Phối hợp với các phòng QH/T, AN/IM, VH/T, TSC... để kiểm tra, khắc phục sự cố, đảm bảo hoạt động xuyên suốt 24/7 của các dịch vụ trọng yếu. 4. Xây dựng quy trình, triển khai dự án và phối hợp kỹ thuật - Xây dựng, cập nhật, chuẩn hóa quy trình vận hành, xử lý sự cố và quản lý các ứng dụng Banking, Thanh toán dịch vụ, Middleware và hệ thống hỗ trợ vận hành. - Tham gia triển khai các dự án CNTT & mua sắm phần mềm, trong đó có Payment Hub, Bank, ACH, DataHub, Middleware, API Gateway, ELK, WLA, CMDB, APOPS... - Điều phối phối hợp nghiệp vụ – kỹ thuật – phát triển phần mềm, quy trình UED, tài liệu phân tích thiết kế, và thử nghiệm nghiệp vụ trước triển khai chức năng. 5. Nghiên cứu, ứng dụng công nghệ mới và đào tạo nội bộ - Nghiên cứu, đánh giá, thử nghiệm (POC) và triển khai các công cụ, giải pháp công nghệ mới phục vụ quản trị, giám sát, tự động hóa vận hành CNTT. - Xây dựng phương án kỹ thuật, tham gia dự án mua sắm và triển khai các hệ thống mới như KMS, EXAMS, PAMS, Proxy, APOPS, CMDB. - Tổ chức đào tạo, hướng dẫn vận hành, chuyển giao công nghệ nội bộ và phối hợp các tiêu chuẩn kỹ thuật cho các bộ kỹ thuật tại TTCNTT và toàn hệ thống BIDV.	≤ 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/nhiệt 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 và 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.	1. Kinh nghiệm: - Có kinh nghiệm quản trị, vận hành các hệ thống phần mềm ứng dụng, nền tảng nền tảng hoặc phần mềm ứng dụng, phần mềm hỗ trợ nền tảng ứng dụng khách hàng. - Đã tham gia triển khai hoặc vận hành các dự án CNTT, ưu tiên ứng viên từng tham gia các dự án CNTT tại BIDV hoặc các tổ chức tài chính, ngân hàng. - Ưu tiên ứng viên có các kinh nghiệm triển khai và quản trị hệ thống ứng dụng trên môi trường Public Cloud (AWS, GCP, Viettel Cloud, CMG Cloud...). 2. Kỹ năng: - Thành thạo quản trị các nền tảng ứng dụng phục vụ triển khai website và dịch vụ số, như WebLogic, WebSphere, JBoss, Tomcat, IIS, Nginx, Apache, các công cụ ETL, dữ liệu, các công cụ của các BL... - Phân tích năng phần mềm, giám sát, tổng hợp báo cáo định kỳ, để xuất biên bản phân tích theo cơ chế an toàn hệ thống. - Có kỹ năng làm việc nhóm, phối hợp với các bộ phận kỹ thuật khác (hạ tầng, bảo mật, phát triển ứng dụng) và chủ động trong nghiên cứu, học hỏi công nghệ mới. - Xây dựng phân tích trên các nền tảng WorkLoad Automation và áp dụng AI trong lĩnh vực Quản trị vận hành các hệ thống CNTT. 3. Chứng chỉ ưu tiên: - Các chứng chỉ CNTT chuyên ngành như: ITIL Foundation, CompTIA Linux+, RHCE, WebLogic/WebSphere Administrator, VMware VCP. - Chứng chỉ Cloud/DevOps như: AWS Certified Solutions Architect, Microsoft Azure Administrator, Google Cloud Professional, Docker/Kubernetes/CKA, OpenAPI, BPM là lợi thế. - Chứng chỉ liên quan đến các nền tảng ETL/BI như: Power BI Data Analyst Associate, IBM Cloud Park for Data System V1.x Administrator Specialty Certified Data Management Professional, Databricks Certified Data Engineer.
Tổng:				10						