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
2	**Chuyên viên bảo mật ứng dụng**	**Chuyên viên bảo mật ứng dụng Cấp 2/3/4**	**Phòng An ninh bảo mật**	**3**	Ngoài hệ thống	**Đánh giá bảo mật ứng dụng (Pentester):** - Thực hiện pentest web/mobile/API, đánh giá cấu hình DB/OS/Container/Cloud theo checklist. - Viết PoC, tái hiện lỗ hổng, đề xuất khắc phục. - Đề xuất xây dựng các quy trình, checklist, tiêu chuẩn về đánh giá bảo mật ứng dụng **An ninh sản phẩm (Product Security):** - Tích hợp secure-by-design vào vòng đời sản phẩm: policy, standard, pattern, library. - Rà soát & chuẩn hóa thư viện/cấu phần bảo mật; tư vấn Secure SDLC cho squad sản phẩm. - Đánh giá rủi ro thay đổi/phiên bản, theo dõi threat intel & lộ trình vá. - Tham gia ý kiến đánh giá đề xuất phương án tăng cường an ninh bảo mật đối với các sản phẩm dịch vụ, hệ thống ứng dụng CNTT tại 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/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.	**Đánh giá bảo mật ứng dụng (Pentester):** - Tối thiểu 2 năm trong công tác đánh giá bảo mật ứng dụng (Pentest); thành thạo Burp/ZAP, Frida/Objection, ADB, mitmproxy, fuzzing cơ bản. - Có hiểu biết về OWASP Top10, API Top10, MASVS, SSRF/RCE/IDOR/Deserialization… - Có khả năng lập trình một số ngôn ngữ phổ biến như Python, Java, C/C++. - Nắm được cách thức thực hiện công việc đánh giá bảo mật theo các quy trình phát triển như Agile, DevSecOps. - Ưu tiên OSCP/OSWE/OSCE/GPEN, có CVE/HoF/CTF nổi bật. **An ninh sản phẩm (Product Security):** - Tối thiểu 2 năm AppSec/Product Security/Secure SDLC; kinh nghiệm làm việc với tribe/squad. - Thành thạo DevSecOps toolchain (SAST/DAST/SCA/Secrets/CICD), risk acceptance. - Có hiểu biết về các lỗ hổng bảo mật ứng dụng (OWASP Top 10, CWE, CVE, …) - Có hiểu biết về DevSecOps, CI/CD pipelines, và quản lý bảo mật trong môi trường container (Docker, Kubernetes) - Có hiểu biết về kiến trúc bảo mật tổng thể cho hệ thống CNTT. - Đánh giá, phân tích và kiểm tra các yêu cầu bảo mật trong quá trình phát triển sản phẩm. Xây dựng các phương án bảo mật cho sản phẩm trước khi đưa vào triển khai chính thức. - Nghiên cứu, xây dựng quy trình, triển khai các công cụ tự động đánh giá, kiểm tra bảo mật phần mềm theo quy trình DevSecOps. - Tham gia rà soát, đánh giá và đề xuất phương án thực hiện đánh giá bảo mật đối với các hệ thống, ứng dụng được triển khai theo các dự án. - Ưu tiên CISSP/GSEC/CSSLP/OSCP, từng dẫn dắt cải tiến bảo mật sản phẩm quy mô lớn.
3	**Chuyên viên GRC**	**Chuyên viên GRC Cấp 2/3/4**	**Phòng An ninh bảo mật**	**2**	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…
4	**Chuyên viên Redteam**	**Chuyên viên Redteam Cấp 2/3/4**	**Phòng An ninh bảo mật**	**1**	Ngoài hệ thống	Kiểm thử xâm nhập các hệ thống ứng dụng CNTT theo hình thức Red Team với các mức độ bảo mật phần mềm khác nhau, từ đó phối hợp với Blue Team nhằm phát hiện, ngăn chặn và khắc phục các lỗ hổng bảo mật. Mô phỏng lại các cuộc tấn công mạng có thật, có thể nhằm vào một sản phẩm hoặc một hệ thống/ đơn vị và thực hiện tất cả các các bước cần thiết mà kẻ tấn công có thể sử dụng. Nắm rõ về những nguy cơ lợi dụng dữ liệu và ngăn chặn việc rò rỉ trong tương lai bằng việc mô tả các cuộc tấn công mạng và các nguy cơ an ninh mạng.	≤ 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 trong công tác kiểm thử xâm nhập (Red Team). - Có khả năng nghiên cứu chuyên sâu, cách debug trên các ngôn ngữ nhằm xây dựng lại mã khai thác liên quan tới các lỗ hổng bảo mật 1-day hay phát hiện các lỗ hổng 0-day - Có hiểu biết về các cơ chế phòng thủ/giám sát của blue-team nhằm tìm cách bypass/ẩn mình trước các cơ chế này. - Hiểu rõ gốc rễ vấn đề (root-cause) của các lỗ hổng bảo mật (theo OWASP, CWE), cách khai thác lỗ hổng thủ công (manual exploit – không sử dụng các công cụ tự động), cách lập trình an toàn (secure coding) và khắc phục lỗi tương ứng. - Hiểu biết về các bước (phase) trong lĩnh vực Red Team. Có kinh nghiệm sử dụng các công cụ hỗ trợ trong quá trình Pentest cũng như các công cụ trong từng Red Team phase. - Có khả năng lập trình một trong những ngôn ngữ kịch bản để viết mã khai thác (Bash, Powershell, Python, Perl, Java, .Net, …), có khả năng sửa, tạo các mã khai thác cho Web, OS, … - Ưu tiên các chứng chỉ bảo mật chuyên sâu như OSCP/OSWE/OSCE/GPEN, có CVE/HoF/CTF nổi bật.
7	**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**	**3**	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 trong yêu: 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 điền 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..	**Ưng 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 báo 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. Có kết quả xếp loại hoàn thành nhiệm vụ từ mức tốt trở lên trong vòng 1 năm gần nhất
Tổng:				**9**						