**PHỤ LỤC: MÔ TẢ CÔNG VIỆC VÀ TIÊU CHUẨN TUYỂN DỤNG CỤ THỂ**

1. **Chuyên gia an ninh bảo mật**
* **Số lượng: 1 người**
* **Nhiệm vụ**
	+ Tham mưu trực tiếp cho lãnh đạo về định hướng, các vấn đề về an ninh bảo mật cho các hệ thống CNTT.
	+ Tư vấn đối với các đơn vị/ cá nhân về các vấn đề bảo mật CNTT khi có yêu cầu.
	+ Phân tích và diễn giải các yêu cầu kinh doanh tương ứng với các yêu cầu về bảo mật. Đưa ra giải pháp kỹ thuật triển khai đáp ứng các yêu cầu bảo mật.
	+ Đánh giá tổng thể về hệ thống bảo mật CNTT, xác định các rủi ro, điểm yếu để đề ra các giải pháp thực hiện.
	+ Xây dựng lộ trình triển khai các giải pháp bảo mật để giải quyết các rủi ro trong hệ thống.
	+ Tham gia thiết kế các giải pháp bảo mật cho hệ thống CNTT theo yêu cầu kinh doanh và các yêu cầu tuân thủ kiến trúc, tiêu chuẩn.
	+ Đánh giá các giải pháp thiết kế (dự án) đảm bảo đáp ứng các yêu cầu về bảo mật.
	+ Đánh giá hoặc đề xuất các yêu cầu bảo mật đến các phần mềm được triển khai.
	+ Phụ trách về kỹ thuật trong quá trình thiết kế, triển khai, và kiểm tra các dự án về an ninh bảo mật CNTT.
	+ Phối hợp với các đơn vị khác để đảm bảo triển khai đúng đắn các giải pháp về bảo mật CNTT.
	+ Nghiên cứu, xây dựng và trình bày các giải pháp bảo mật mới cho lãnh đạo.
	+ Xây dựng và phát triển các chỉ tiêu, thông số đo lường về hệ thống bảo mật CNTT.
	+ Tham gia vào việc xử lý các sự cố bảo mật ở cấp độ nghiêm trọng.
	+ Đào tạo về an ninh bảo mật cho các cán bộ kỹ thuật.
	+ Nghiên cứu, xây dựng các chương trình đào tạo về bảo mật theo các cấp độ khác nhau đối với cán bộ kỹ thuật và cán bộ nghiệp vụ.
	+ Trực tiếp tham gia đào tạo về lĩnh vực bảo mật theo chương trình được phê duyệt và khi có yêu cầu.
	+ Tổ chức cập nhật công nghệ mới về bảo mật cho các cán bộ.
	+ Tham gia vào các hoạt động nhằm nâng cao kiến thức, ý thức cho cán bộ về bảo mật bao gồm: tham gia viết bài đăng tải trên Intranet, tạp chí nội bộ, tổ chức các buổi hội thảo về công tác bảo mật.
* **Yêu cầu**
	+ Kinh nghiệm tối thiểu 5 năm trong lĩnh vực chuyên môn CNTT.
	+ Đạt được một trong số các chứng chỉ: chứng chỉ bảo mật cơ bản CEH/CHFI; chứng chỉ bảo mật OSCP/OSWE/OSCE; chứng chỉ bảo mật nâng cao CISSP/CISA/các chứng chỉ của GIAC.
	+ Có kiến thức về hệ thống CNTT, phần mềm, phần cứng, về mạng máy tính và bảo mật CNTT.
	+ Có kiến thức sâu về các giải pháp, thiết bị bảo mật (mạng, phần cứng, phần mềm ứng dụng) và phòng ngừa rủi ro CNTT.
	+ Có hiểu biết rộng về các hệ thống CNTT: Phần cứng, phần mềm, hệ thống Website, hệ thống mạng truyền thông,…
	+ Có khả năng thực hiện và đề xuất giải pháp quản trị, xử lý các sự cố một cách khoa học đối với hệ thống bảo mật CNTT.
	+ Có khả năng nghiên cứu và đề xuất áp dụng các giải pháp bảo mật CNTT; Có khả năng phân tích, kiểm soát, đánh giá rủi ro đối với các vấn đề về bảo mật.
1. **Chuyên viên quản trị hệ thống bảo mật**
* **Số lượng: 1 người**
* **Nhiệm vụ**
	+ Quản trị các hệ thống an ninh bảo mật.
	+ Cấu hình và thiết lập chính sách bảo mật cho các hệ thống an ninh bảo mật.
	+ Tham gia xây dựng, triển khai các dự án, kế hoạch mua sắm liên quan tới an ninh bảo mật.
	+ Tham gia xây dựng và cập nhật quy trình, quy định, chính sách bảo mật.
	+ Tham gia thực hiện triển khai các quy trình, chính sách an ninh an toàn thông tin.
* **Yêu cầu**
	+ Có kiến thức về hệ thống CNTT, hệ điều hành, phần cứng, mạng truyền thông và bảo mật CNTT.
	+ Nắm vững cơ chế, quy chế, quy trình, quy định của Nhà nước về bảo mật thông tin.
	+ Có kiến thức cơ bản về luật pháp.
	+ Có kỹ năng giải quyết vấn đề.
	+ Có kỹ năng lập kế hoạch và viết các báo cáo đề xuất.
1. **Chuyên viên rà soát, quản lý lỗ hổng**
* **Số lượng: 2 người**
* **Nhiệm vụ**
	+ Đánh giá an toàn bảo mật cho các hệ thống CNTT quan trọng.
	+ Thực hiện công tác kiểm tra đánh giá tuân thủ an ninh an toàn thông tin trong nội bộ.
	+ Tham gia thực hiện triển khai các quy trình, chính sách an ninh an toàn thông tin.
	+ Tham gia xây dựng, triển khai các dự án, kế hoạch mua sắm liên quan tới an ninh bảo mật.
	+ Quản trị các hệ thống an ninh bảo mật về đánh giá an toàn bảo mật.
	+ Cấu hình và thiết lập chính sách bảo mật cho các hệ thống an ninh bảo mật về đánh giá an toàn bảo mật.
* **Yêu cầu**
	+ Có kiến thức về hệ thống CNTT, hệ điều hành, phần cứng, mạng truyền thông và bảo mật CNTT.
	+ Nắm vững cơ chế, quy chế, quy trình, quy định của Nhà nước về bảo mật thông tin.
	+ Có kiến thức cơ bản về luật pháp.
	+ Có kỹ năng giải quyết vấn đề.
	+ Có kỹ năng lập kế hoạch và viết các báo cáo đề xuất.
1. **Chuyên viên an ninh sản phẩm**
* **Số lượng: 2 người**
* **Nhiệm vụ**
	+ Đánh giá an toàn bảo mật cho các sản phẩm CNTT trong toàn bộ quá trình phát triển sản phẩm từ khâu phân tích thiết kế tới khi nghiệm thu, triển khai.
	+ Phối hợp thực hiện công tác kiểm tra đánh giá tuân thủ an ninh an toàn thông tin trong nội bộ.
	+ Tham gia thực hiện triển khai các quy trình, chính sách an ninh an toàn thông tin.
	+ Tham gia xây dựng, triển khai các dự án, kế hoạch mua sắm liên quan tới an ninh bảo mật.
* **Yêu cầu**
	+ Có kiến thức về hệ thống CNTT, hệ điều hành, phần cứng, mạng truyền thông và bảo mật CNTT.
	+ Nắm vững cơ chế, quy chế, quy trình, quy định của Nhà nước về bảo mật thông tin.
	+ Có kiến thức cơ bản về luật pháp.
	+ Có kỹ năng giải quyết vấn đề.
	+ Có kỹ năng lập kế hoạch và viết các báo cáo đề xuất.
1. **Chuyên viên Bảo mật mạng – máy tính**
* **Số lượng: 1 người**
* **Nhiệm vụ**
	+ Quản trị các hệ thống an ninh bảo mật.
	+ Cấu hình và thiết lập chính sách bảo mật cho các hệ thống an ninh bảo mật.
	+ Tham gia xây dựng, triển khai các dự án, kế hoạch mua sắm liên quan tới an ninh bảo mật.
	+ Tham gia xây dựng và cập nhật quy trình, quy định, chính sách bảo mật.
	+ Tham gia thực hiện triển khai các quy trình, chính sách an ninh an toàn thông tin.
* **Yêu cầu**
	+ Có kiến thức về hệ thống CNTT, hệ điều hành, phần cứng, mạng truyền thông và bảo mật CNTT.
	+ Nắm vững cơ chế, quy chế, quy trình, quy định của Nhà nước về bảo mật thông tin.
	+ Có kiến thức cơ bản về luật pháp.
	+ Có kỹ năng giải quyết vấn đề.
	+ Có kỹ năng lập kế hoạch và viết các báo cáo đề xuất.
1. **Chuyên viên Bảo mật Red Team**
* **Số lượng: 4 người**
* **Nhiệm vụ**
	+ Công việc của Red Team tập trung vào việc kiểm thử xâm nhập ở các hệ thống với các mức độ bảo mật phần mềm khác nhau, phát hiện, ngăn chặn và khắc phục các lỗ hổng bảo mật.
	+ Red Team mô phỏng lại các cuộc tấn công có thật, có thể nhắm 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. Bằng việc đóng vai một kẻ tấn công, Red Team cho thấy được những lỗ hổng bảo mật hoặc các “cửa hậu” có thể bị lợi dụng để đe dọa an ninh mạng.
	+ 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 minh mạng.
* **Yêu cầu**
	+ 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 (Bắt buộc).
	+ 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, …
	+ 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 là một lợi thế.
	+ 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 là một lợi thế.
	+ Từng tham gia, đạt giải các cuộc thi về ATTT, CTF là một lợi thế.
	+ Tham gia các chương trình bug bounty, có các CVE hay có các bài viết phân tích các lỗ hổng bảo mật chuyên sâu là một lợi thế.
	+ Có khả năng đọc hiểu Tiếng Anh đủ tốt cho các tài liệu chuyên ngành.
	+ Có những chứng chỉ liên quan đến Pentest, Redteam như OSCE/OSWE/OSCP/GPEN, … là một lợi thế.
	+ Có khả năng làm việc độc lập, có tính tự giác, chủ động trong công việc.
1. **Chuyên viên Theo dõi 24x7 (thuộc Blue Team)**
* **Số lượng: 7 người**
* **Nhiệm vụ**
	+ Giám sát trạng thái an ninh của toàn bộ hệ thống công nghệ thông tin theo thời gian thực trên một giao diện quản lí tập trung duy nhất.
	+ Giám sát, phát hiện và cảnh báo bất thường tại từng nút mạng hoặc trên từng thiết bị.
	+ Phân tích và cảnh báo sớm các điểm yếu, nguy cơ an ninh có thể xảy ra.
	+ Hỗ trợ ứng cứu và xử lí các sự cố an ninh mạng.
	+ Xử lý các sự kiện theo qui trình nghiệp vụ, tự động hóa trong công tác vận hành hệ thống.
* **Yêu cầu**
	+ Có kiến thức về hệ thống CNTT, hệ điều hành, phần cứng, mạng truyền thông và bảo mật CNTT.
	+ Nắm vững cơ chế, quy chế, quy trình, quy định của Nhà nước, ngành, BIDV về bảo mật thông tin.
	+ Có kiến thức cơ bản về luật pháp.
	+ Có kỹ năng giải quyết vấn đề.
	+ Có khả năng làm việc theo nhóm.
	+ Nhiệt tình trong công việc.
1. **Chuyên viên Phân tích sự kiện bảo mật (forensic Team)**
* **Số lượng: 2 người**
* **Nhiệm vụ**
	+ Có chức năng chủ động rà quét, săn tìm các sự cố bảo mật.
	+ Phân tích mã độc.
	+ 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.
* **Yêu cầu**
	+ Có tính chủ động, có khả năng tư duy, tự nghiên cứu, đọc hiểu các tài liệu chuyên ngành liên quan tới các giải pháp an ninh bảo mật.
	+ Có tư duy về lập trình, có thể sử dụng ít nhất một trong những ngôn ngữ lập trình như JS, Python, Java, …
	+ Có hiểu biết về các kỹ thuật tấn công, có khả năng xây dựng giả lập các tấn công theo các phase trong cyber kill chain là một lợi thế.
	+ Có khả năng đọc hiểu Tiếng Anh đủ tốt cho các tài liệu chuyên ngành.
	+ Có một trong các chứng chỉ liên quan đến Malware Analysis, Incident response, Forensic là một lợi thế.
	+ Có khả năng làm việc độc lập, có tính tự giác, chủ động trong công việc.
1. **Chuyên viên Quản lý chất lượng**
* **Số lượng: 10 người**
* **Nhiệm vụ**
	+ Thực hiện công tác kiểm tra, nghiệm thu các phần mềm mới/nâng cấp/bảo trì được bàn giao từ Khối phát triển
	+ Tham gia xây dựng kế hoạch kiểm thử (Test Plan)
	+ Tham gia xây dựng Bộ kịch bản kiểm thử (Test Case); Chuẩn bị môi trường, dữ liệu kiểm thử; Chuẩn bị Test script (trường hợp sử dụng Automation Test); Kiểm thử hiệu năng ứng dụng; Theo dõi việc xử lý lỗi của đội phát triển và tổng hợp báo cáo tiến độ kiểm thử, các vướng mắc lên Lãnh đạo phòng/Quản trị dự án.
	+ Tham gia xây dựng, hoàn thiện các tài liệu dự án liên quan đến toàn bộ quá trình kiểm thử.
* **Yêu cầu**
	+ Có trình độ đại học trở lên, chuyên ngành Công nghệ Thông tin.
	+ Có hiểu biết về quy trình kiểm thử, quy trình phát triển phần mềm, các phương pháp phát triển phần mềm phổ biến (Waterfall, Agile/DevOps).
	+ Có hiểu biết về các phương pháp kiểm thử thủ công (Manual test) và/hoặc kiểm thử tự động (Automation test), các công cụ quản lý phục vụ cho quá trình kiểm tra, nghiệm thu, tham gia được vào các hoạt động và tiến trình kiểm thử phần mềm.
	+ Có khả năng làm việc độc lập hoặc theo nhóm, cẩn thận, tỉ mỉ, có kỹ năng lập kế hoạch, xây dựng các báo cáo công việc định kỳ/đột xuất.

**\* Ưu tiên:**

* + Có hiểu biết và kinh nghiệm từ 01 năm về các kỹ thuật kiểm thử tự động, các công cụ phục vụ kiểm thử tự động, có khả năng viết và thực hiện các Test script, xây dựng Framework kiểm thử tự động.
	+ Có hiểu biết và nắm bắt việc cài đặt, quản trị, sử dụng một số công nghệ nền tảng như: PL/SQL, IBM COGNOS, IBM Portal và IBM Web, Apache Tomcat, Web Service, API,..., có hiểu biết và kỹ năng xử lý về cơ sở dữ liệu như Oracle, SQL Server, DB2…
	+ Có hiểu biết về nghiệp vụ ngân hàng và các hệ thống phần mềm của ngân hàng.