PHỤ LỤC V

ĐỊNH MỨC KINH TẾ - KỸ THUẬT ĐIỀU PHỐI GIÁM SÁT HỆ THỐNG SOC VÀ CÁC CÔNG TÁC AN TOÀN BẢO MẬT CÁC HỆ THỐNG THÔNG TIN CỦA THÀNH PHỐ

(Ban hành kèm theo Quyết định số /2025/QĐ-UBND ngày tháng năm 2025)

HNI.05.00.00. Điều phối giám sát hệ thống SOC và các công tác an toàn bảo mật các hệ thống thông tin của thành phố

HNI.05.01.00. Quản lý, vận hành Trung tâm giám sát an toàn thông tin của thành phố (SOC)

HNI.05.01.01. Vận hành

a) Thành phần công việc

- Thực hiện các nghiệp vụ quản lý, vận hành.
  - Quản lý vận hành bảo đảm các hoạt động bình thường toàn bộ hạ tầng của hệ thống.
  - Theo dõi, thường xuyên, liên tục trạng thái hoạt động của hệ thống, tài nguyên, băng thông, trạng thái kết nối để bảo đảm hệ thống hoạt động bình thường, có tính sẵn sàng cao, thu thập thông tin ổn định, liên tục.
  - Theo dõi, cập nhật thông tin các hướng dẫn, cảnh báo lỗ hổng bảo mật của Bộ Thông tin và Truyền thông.
  - Theo dõi, giám sát các sự kiện, tấn công mạng ghi nhận được trên hệ thống.
  - Thu thập, xử lý, phân tích log.
  - Truy xuất dữ liệu phục vụ phân tích tấn công.
- Giám sát, theo dõi, cập nhật cảnh báo tình trạng hoạt động.
  - Giám sát, theo dõi và cảnh báo ở lớp mạng.
  - Giám sát, theo dõi và cảnh báo lớp máy chủ.
  - Giám sát, theo dõi và cảnh báo lớp ứng dụng.
  - Giám sát, theo dõi và cảnh báo lớp thiết bị đầu cuối.
  - Giám sát an toàn thông tin và phòng thủ mã độc.
- Đánh giá, phân loại sự cố và thực hiện cảnh báo sự cố.
- Hỗ trợ kỹ thuật, giải đáp thắc mắc, khó khăn khi vận hành.
- Giám sát, kiểm tra việc sao lưu dữ liệu.
- Bàn giao ca trực và các nội dung về sự cố, công việc còn tồn đọng.

- Cập nhật thông tin ca trực (thành viên, thời gian ca trực, các sự vụ trong ca…).

b) Định mức

Đơn vị tính: Hệ thống/ngày làm việc

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
HNI.05.01.01	*Nhân công*		
	Kỹ sư bậc 3	Công	0,458
	Kỹ sư bậc 4	Công	4,292
	Kỹ sư bậc 5	Công	3,865
	Máy, thiết bị		
	Máy tính xách tay	Ca	8,615

HNI.05.01.02. Khắc phục sự cố

a) Thành phần công việc

- Sao lưu, back up dữ liệu trước khi xử lý sự cố.
- Ghi chép, lưu trữ thông số, trạng thái hệ thống.
- Kiểm tra các phần mềm, thông số, cấu hình, thiết lập.
- Xử lý sự cố kỹ thuật liên quan đến hệ thống.
    - Thực hiện đầy đủ các bản vá, các hướng dẫn, cảnh báo lỗ hổng bảo mật của Bộ Thông tin và Truyền thông.
    - Tiếp nhận cảnh báo, xác minh và thực hiện các hành động để xử lý sự cố.
    - Xác định các hành động ứng cứu khẩn cấp: Phản ứng chặn kênh kết nối điều khiển, bổ sung luật ngăn chặn sớm tấn công hoặc cô lập hệ thống.
    - Tiến hành phân loại nguy cơ, rủi ro, sự cố an toàn thông tin mạng.
    - Xử lý các lỗ hổng, điểm yếu, cập nhật bản vá và bóc gỡ mã độc trên hệ thống.
    - Ngăn chặn tấn công.
    - Thiết lập lại, khôi phục các thông số cài đặt, cấu hình, nâng cấp (nếu có thể) các cài đặt.
- Kiểm tra, chạy thử.
- Ghi nhận hoạt động của hệ thống và nhật ký xử lý sự cố.
- Lập báo cáo sự cố, lưu hồ sơ thông tin sự cố (thời gian khắc phục xong, nguyên nhân và phương án xử lý…).

b) Định mức

Đơn vị tính: Sự cố

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
HNI.05.01.02	*Nhân công*		
	Kỹ sư bậc 3	Công	1,875
	Kỹ sư bậc 4	Công	5,188
	Kỹ sư bậc 5	Công	6,208
	Vật liệu		
	Giấy A4	Ram	0,030
	Bút	Cái	0,020
	Mực in	Hộp	0,005
	Máy, thiết bị		
	Máy tính	Ca	0,073
	Máy tính xách tay	Ca	13,198
	Máy in	Ca	0,004

HNI.05.02.00. Điều phối hoạt động ứng cứu sự cố an toàn thông tin mạng của các cơ quan Đảng, Nhà nước, tổ chức chính trị-xã hội trên địa bàn thành phố

HNI.05.02.01. Sự cố an toàn thông tin thông thường

a) Thành phần công việc

- Tiếp nhận thông tin sự cố: Tiếp nhận thông tin từ nhiều nguồn (hệ thống theo dõi nội bộ, đơn vị chuyên trách, nguồn tin xã hội, tổ chức ứng cứu hoặc nguồn khác).
- Phân tích, xác minh phân loại sự cố.
  - Thu thập thông tin về sự cố.
  - Phân tích, nhận định phạm vi, đối tượng bị ảnh hưởng.
  - Xác minh các thông tin về tình trạng, loại, mức độ, phạm vi ảnh hưởng, đối tượng và địa điểm xảy ra sự cố.
- Phân tích, lựa chọn phương án ứng cứu sự cố.
- Triển khai phương án ứng cứu ban đầu.
  - Xác định phạm vi, đối tượng, mục tiêu cần ứng cứu sự cố.
  - Thực hiện các khảo sát về kiến trúc, mô hình, hạ tầng mạng, hệ điều hành, các thiết bị và ứng dụng có liên quan…
  - Xây dựng phương án ứng cứu dựa trên kết quả khảo sát.

- Điều phối công tác ứng cứu.

- Triển khai phương án ứng cứu khẩn cấp.

- Xử lý sự cố, gỡ bỏ.
- Khôi phục hệ thống.
- Kiểm tra đánh giá lại hệ thống.

- Tổng kết, đánh giá: Xây dựng báo cáo tổng kết ứng phó sự cố. Đúc rút kinh nghiệm.

b) Định mức

Đơn vị tính: Sự cố

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
HNI.05.02.01	*Nhân công*		
	Kỹ sư bậc 3	Công	6,396
	Kỹ sư bậc 4	Công	7,417
	Kỹ sư bậc 5	Công	7,833
	Vật liệu		
	Giấy A4	Ram	0,060
	Bút	Cái	0,050
	Mực in	Hộp	0,030
	Máy, thiết bị		
	Máy tính	Ca	10,875
	Máy tính xách tay	Ca	10,771
	Máy chủ	Ca	6,000
	Hệ thống ảo hóa máy chủ	Ca	6,000
	Hệ thống phát hiện và ngăn chặn xâm nhập	Ca	6,000
	Hệ thống giám sát mạng	Ca	6,000
	Hệ thống tường lửa ứng dụng web	Ca	6,000
	Hệ thống rà quét lỗ hổng	Ca	6,000
	Hệ thống rà quét mã độc	Ca	6,000
	Máy in	Ca	0,010

HNI.05.02.02. Sự cố an toàn thông tin nghiêm trọng

a) Thành phần công việc

- Phát hiện, tiếp nhận sự cố (hệ thống theo dõi nội bộ, đơn vị chuyên trách, tổ chức ứng cứu…).

- Xác minh, phân tích, đánh giá và phân loại sự cố.

- Thu thập thông tin về sự cố.
- Xác minh, phân tích, đánh giá và phân loại sự cố.
- Phân tích, nhận định phạm vi, đối tượng bị ảnh hưởng.

- Xác định các phương án ứng cứu.

- Lựa chọn phương án ứng cứu.

- Phân tích, lựa chọn phương án ứng cứu khẩn cấp.

- Phân tích, lựa chọn phương án ứng cứu khẩn cấp quốc gia.
- Triệu tập bộ phận tác nghiệp ứng cứu khẩn cấp để ứng cứu, xử lý sự cố.
- Phân công nhiệm vụ triển khai các biện pháp ứng cứu khẩn cấp.

- Triển khai phương án ứng cứu ban đầu.

- Xác định phạm vi, đối tượng, mục tiêu cần ứng cứu và dự đoán diễn biến.
- Thực hiện các khảo sát về kiến trúc, mô hình, hạ tầng mạng, hệ điều hành, các thiết bị và ứng dụng có liên quan…
- Xây dựng phương án ứng cứu dựa trên kết quả khảo sát.
- Điều phối các hoạt động ứng cứu ban đầu.
- Cảnh báo sự cố trên mạng lưới ứng cứu quốc gia.
- Tiến hành các biện pháp khôi phục tạm thời.
- Xử lý hậu quả ban đầu.
- Ngăn chặn, xử lý các hành vi đã được phát hiện.

- Triển khai phương án ứng cứu khẩn cấp.

- Ứng cứu ngăn chặn sự cố.
- Thu thập thông tin sự cố (chứng cứ).
- Phân tích, điều tra chứng cứ.
- Khắc phục sự cố, gỡ bỏ mã độc.
- Ngăn chặn, xử lý hậu quả.
- Xác minh nguyên nhân và truy tìm nguồn gốc.
- Kiểm tra, đánh giá hệ thống thông tin.

- Tổng kết, đánh giá: Xây dựng báo cáo tổng kết ứng phó sự cố. Đúc rút kinh nghiệm.

b) Định mức

Đơn vị tính: Sự cố

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
HNI.05.02.02	*Nhân công*		
	Kỹ sư bậc 3	Công	13,102
	Kỹ sư bậc 4	Công	17,100
	Kỹ sư bậc 5	Công	20,875
	Vật liệu		
	Giấy A4	Ram	0,120
	Bút	Cái	0,050
	Mực in	Hộp	0,060
	Máy, thiết bị		
	Máy tính	Ca	25,371
	Máy tính xách tay	Ca	25,706
	Máy chủ	Ca	9,000
	Hệ thống ảo hóa máy chủ	Ca	9,000
	Hệ thống phát hiện và ngăn chặn xâm nhập	Ca	9,000
	Hệ thống giám sát mạng	Ca	9,000
	Hệ thống tường lửa ứng dụng web	Ca	9,000
	Hệ thống rà quét lỗ hổng	Ca	9,000
	Hệ thống rà quét mã độc	Ca	9,000
	Máy in	Ca	0,010

HNI.05.03.00. Kiểm tra, đánh giá, phát hiện lỗ hổng bảo mật, điểm yếu an toàn thông tin cho các cơ quan nhà nước

a) Thành phần công việc

- Xây dựng kế hoạch thực hiện.

- Thu thập hồ sơ, tài liệu về hệ thống cần đánh giá: các dữ liệu cần thiết cho việc đánh giá bảo mật như: Domain Names, Server Names, IP Addresses, Network Map, ISP/ASP information, System and Service Owners, OS Identification, Port scanning, Services identification…

- Thực hiện dò quét, kiểm tra, phân tích, đánh giá để tìm và phát hiện các lỗ hổng tồn tại trên các máy chủ từ bên ngoài như phiên bản hệ điều hành, các cổng dịch vụ đang mở, hệ thống firewall bảo vệ, khả năng đáp ứng dịch vụ của máy chủ…

- Thực hiện các tấn công thử nghiệm để kết luận các lỗ hổng thực sự nguy hiểm tới hệ thống.

- Thực hiện các phân tích, đánh trọng số, phân loại lỗ hổng và tạo các bản báo cáo cuối cùng cho cơ quan/đơn vị.

- Xây dựng báo cáo đánh giá.

b) Định mức

Đơn vị tính: Hệ thống

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
HNI.05.03.00	*Nhân công*		
	Kỹ sư bậc 3	Công	0,281
	Kỹ sư bậc 4	Công	0,510
	Vật liệu		
	Giấy A4	Ram	0,100
	Bút	Cái	0,100
	Mực in	Hộp	0,025
	Máy, thiết bị		
	Máy tính	Ca	0,281
	Máy tính xách tay	Ca	0,510
	Hệ thống rà quét lỗ hổng	Ca	0,135
	Máy in	Ca	0,013

HNI.05.04.00. Thu thập, phân tích và cảnh báo nguy cơ, sự cố tấn công mạng cho các cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội trên địa bàn thành phố

a) Thành phần công việc

- Thu thập thông tin giám sát và nghiên cứu hệ thống giám sát.

  - Thu thập thông tin về các hệ thống thông tin của đơn vị cơ quan nhà nước trên địa bàn thành phố.
  - Nghiên cứu mạng lưới giám sát an toàn thông tin mạng, liên kết, liên thông giữa các trung tâm giám sát an toàn không gian mạng quốc gia với các tổ chức, doanh nghiệp.

- Giám sát: Giám sát tập trung hệ thống kỹ thuật, mạng lưới an toàn thông tin, tấn công mạng, kết nối, truy nhập, xâm nhập, phần mềm độc hại.

- Thu thập, phân loại, tổng hợp thông tin.

- Thu thập, phân loại thông tin nguy cơ tấn công mạng từ hoạt động giám sát.
- Thu thập, phân loại thông tin mất quyền điều khiển; phần mềm độc hại, yếu tố nghẽn băng thông, nguy cơ tấn công mạng.

- Phân tích thông tin.
  - Loại bỏ dữ liệu, thông tin vô nghĩa, trùng lặp.
  - Bóc tách, phân loại dữ liệu, thông tin và dự báo về nguy cơ, tấn công mạng (nghiêm trọng, cao, trung bình, thấp) và đối tượng bị ảnh hưởng.
  - Phân tích để tìm ra các nguy cơ tấn công mạng.
  - Đánh giá mức độ ảnh hưởng, tác động của thông tin giám sát, thu thập được.
  - Đánh giá đối tượng bị ảnh hưởng.
- Đề xuất phương án dự báo, cảnh báo và xử lý nguy cơ.
  - Nghiên cứu các nguy cơ, xây dựng giải pháp.
  - Xây dựng phương án hỗ trợ kiểm tra, phương án xử lý.
  - Hướng dẫn chuyên sâu về xử lý nguy cơ, tấn công mạng; hỗ trợ kiểm tra, xử lý nguy cơ, tấn công mạng.
- Phát hành dự báo, cảnh báo sớm tới các đối tượng liên quan.
- Tổng kết, xây dựng báo cáo đánh giá.

b) Định mức

Đơn vị tính: Ngày

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
HNI.05.04.00	*Nhân công*		
	Kỹ sư bậc 3	Công	0,229
	Kỹ sư bậc 4	Công	0,479
	Vật liệu		
	Giấy A4	Ram	0,050
	Bút	Cái	0,050
	Mực in	Hộp	0,025
	Máy, thiết bị		
	Máy tính	Ca	0,229
	Máy tính xách tay	Ca	0,479
	Hệ thống phân tích và chia sẻ nguy cơ tấn công mạng	Ca	0,031

	Hệ thống xử lý các nguồn dữ liệu	Ca	0,021
	Máy in	Ca	0,021

HNI.05.05.00. Diễn tập phòng chống tấn công mạng đảm bảo an toàn thông tin cho các lĩnh vực quan trọng của địa phương

a) Thành phần công việc

- Xác định đối tượng diễn tập.
  - Trao đổi thông tin về nhu cầu tổ chức diễn tập.
  - Xây dựng phiếu điều tra khảo sát nhu cầu diễn tập và thực hiện khảo sát; xử lý, phân tích thông tin thu thập.
  - Báo cáo khảo sát, đánh giá, phân loại người diễn tập.
- Xác định hệ thống diễn tập theo các cấp độ an toàn thông tin.
- Xác định chủ đề diễn tập.
  - Chủ đề về mã độc:

    Phân tích mã độc ở mức traffic và tìm kiếm các hành vi, dấu hiệu, cách thức phát hiện mã độc trong mạng, phục vụ công tác ứng cứu sự cố nhanh.

    Phân tích mã độc ở mức chuyên sâu.
  - Xác định chủ đề tấn công từ chối dịch vụ (tấn công cạn kiệt tài nguyên, tấn công tràn băng thông).
- Xây dựng các phương án, kịch bản.
  - Xây dựng phương án triển khai:
  - Xây dựng kịch bản diễn tập.

    Xây dựng môi trường, công cụ thử nghiệm.

    Lựa chọn phương thức tấn công, vật mẫu tấn công, thiết kế chức năng mẫu mã độc làm kịch bản.

    Demo tấn công, sự cố trên môi trường thử nghiệm.

    Đánh giá, hiệu chỉnh, môi trường, vật mẫu.

    Diễn tập thử nghiệm kịch bản, thu thập các thông tin liên quan phục vụ quá trình xây dựng kịch bản chính thức và diễn tập.

    Sửa chữa, điều chỉnh kịch bản nếu có.
- Kiểm thử phương án, kịch bản trên môi trường thực tế diễn tập.
- Cài đặt, chạy thử hệ thống.
  - Cài đặt hệ thống, phần mềm, thiết bị chính phục vụ diễn tập.
  - Tiến hành kiểm tra chạy thử hệ thống, phần mềm, thiết bị chính phục vụ diễn tập.

- Tiến hành kiểm tra chạy thử kỹ thuật, phối hợp giữa tất cả các hệ thống.
- Cài đặt, chạy thử phương án theo kịch bản.
- Cài đặt phương án, các bước theo kịch bản diễn tập.

- Tiến hành kiểm tra, chạy thử phương án theo kịch bản diễn tập.
- Thực hiện diễn tập theo các bước.
  - Khởi động và duy trì hệ thống diễn tập.
  - Cập nhật thông tin các đội tham gia diễn tập.
  - Giới thiệu và hướng dẫn kịch bản diễn tập.
  - Theo dõi, giám sát quá trình diễn tập.
  - Tiếp nhận và xử lý các yêu cầu của các đơn vị tham gia.
  - Giải đáp ý kiến của các đội về tình huống, kịch bản...
- Tổng kết: Lập phiếu đánh giá, tổng hợp kết quả và báo cáo quá trình diễn tập.

b) Định mức

Đơn vị tính: Cuộc diễn tập

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
HNI.05.05.00	*Nhân công*		
	Kỹ sư bậc 3	Công	36,646
	Kỹ sư bậc 4	Công	21,733
	Kỹ sư bậc 5	Công	28,104
	Vật liệu		
	Giấy A4	Ram	0,250
	Bút	Cái	0,150
	Mực in	Hộp	0,125
	Máy, thiết bị		
	Máy tính	Ca	9,438
	Máy tính xách tay	Ca	63,108
	Máy chủ	Ca	12,000
	Hệ thống ảo hóa máy chủ	Ca	12,000
	Hệ thống phát hiện và ngăn chặn xâm nhập	Ca	12,000
	Hệ thống rà quét lỗ hổng	Ca	12,000

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
	Hệ thống quản lý sự kiện tập trung	Ca	12,000
	Máy in	Ca	0,031

HNI.05.06.00. Giám sát an toàn thông tin cho các lĩnh vực quan trọng và hệ thống thông tin phục vụ Chính quyền điện tử

HNI.05.06.01. Giám sát trực tiếp

a) Thành phần công việc

- Tiếp nhận thông tin giám sát.
  - Tiếp nhận thông tin về địa điểm, phạm vi cần được giám sát; Tiếp nhận thông tin về nguy cơ mất an toàn thông tin, sự cố an toàn thông tin từ đơn vị, các chủ quản/sử dụng hệ thống thông tin; Tiếp nhận thông tin từ các chuyên gia.
  - Lên phương án, triển khai đặt thiết bị giám sát tại địa điểm giám sát; theo dõi, trực giám sát đảm bảo thiết bị quan trắc và hệ thống giám sát trung tâm hoạt động và tiếp nhận dữ liệu ổn định theo đúng quy định.
- Tổng hợp, phân loại thông tin, dữ liệu thu thập được.
  - Tổng hợp số liệu về các sự kiện bất thường dựa trên dữ liệu thu thập được từ các thiết bị quan trắc.
  - Phân loại các sự kiện cảnh báo dựa trên dữ liệu thu thập được từ thiết bị quan trắc để phân loại ra các mức độ nguy hiểm khác nhau.
  - Nghiên cứu, đánh giá thông tin thu thập.
- Kiểm tra, phân tích chứng cứ, dữ liệu để phát hiện bất thường.
- Điều tra, xác minh nhằm xác định nguy cơ, sự cố xảy ra với đối tượng giám sát.
  - Trao đổi thông tin với đơn vị, cá nhân chủ quản hệ thống thông tin để xác minh nguy cơ, sự cố có thể tác động lên hệ thống.
  - Nghiên cứu, điều tra xác minh các nguy cơ, sự cố.
- Xem xét nguy cơ mất an toàn thông tin hoặc sự cố an toàn thông tin.
  - Nghiên cứu dữ liệu phân tích và thông tin xác nhận từ đơn vị, cá nhân chủ quản/sử dụng hệ thống thông tin để đánh giá nguy cơ mất an toàn thông tin hay sự cố an toàn thông tin của hệ thống thông tin.
  - Đánh giá mức độ ảnh hưởng tác động lên hệ thống thông tin: đánh giá nguy cơ bên ngoài và mức độ ảnh hưởng tác động lên hệ thống; đánh giá nguy cơ bên trong và mức độ ảnh hưởng tác động lên hệ thống.

- Phân tích chuyên sâu, phân loại rủi ro, sự cố an toàn thông tin.

- Phân loại rủi ro, sự cố an toàn thông tin.
- Xác định điểm yếu tồn tại; phân tích chuyên sâu để xác định phương thức, thủ đoạn, cách thức tấn công, nguồn tấn công, mục tiêu tấn công, mục đích tấn công.
- Thực nghiệm trong môi trường giả lập để xác định phương thức, thủ đoạn, cách thức tấn công, nguồn tấn công, mục tiêu tấn công, mục đích tấn công.
- Thực nghiệm trực tiếp trên hệ thống thông tin được giám sát để xác định phương thức, cách thức tấn công; xác định mục tiêu, mục đích tấn công.
- Đánh giá mức độ nghiêm trọng, thiệt hại.

- Thực hiện cảnh báo với đơn vị, cá nhân chủ quản hệ thống thông tin.

- Thực hiện cảnh báo nguy cơ mất an toàn thông tin/sự cố an toàn thông tin với đơn vị, cá nhân chủ quản/sử dụng hệ thống thông tin và lập báo cáo cảnh báo.

- Xem xét, đề xuất phương án xử lý, xin chỉ thị cấp trên.

- Nghiên cứu, đề xuất phương án xử lý nguy cơ/sự cố an toàn thông tin và báo cáo lãnh đạo và xin chỉ thị trong trường hợp đơn vị, cá nhân chủ quản/sử dụng hệ thống thông tin không xử lý được nguy cơ mất an toàn thông tin hoặc sự cố an toàn thông tin và có yêu cầu nhờ hỗ trợ xử lý và Báo cáo xin chỉ thị của lãnh đạo cấp trên.

- Xử lý nguy cơ, sự cố xảy ra với đối tượng giám sát: Thiết lập biện pháp kỹ thuật xử lý các nguy cơ/ sự cố xảy ra với đối tượng giám sát.

- Thiết lập biện pháp kỹ thuật xử lý các nguy cơ/ sự cố xảy ra với hệ thống mạng.
- Thiết lập biện pháp kỹ thuật xử lý các nguy cơ/ sự cố xảy ra với đối tượng giám sát.

- Tiếp tục theo dõi nhằm xác định nguy cơ, sự cố xảy ra với đối tượng giám sát.

- Theo dõi nguy cơ/ sự cố an toàn thông tin đã được xử lý nhằm đảm bảo nguy cơ, sự cố đã được xử lý triệt để trên hệ thống thông tin được giám sát; Theo dõ phát hiện dấu hiệu, sự kiện bất thường trên thiết bị quan trắc.
- Đề xuất phương án, xử lý các sự cố phát sinh.

- Cập nhật, điều chỉnh hệ thống giám sát định kỳ.

- Nghiên cứu, cập nhật các diễn biến mới về tình hình an toàn thông tin.

- Phân loại, phân tích các lỗ hổng bảo mật, mã độc, các phương thức tấn công mạng mới và đưa ra nhận định mức độ ảnh hưởng đối hệ thống thông tin đang được giám sát.

- Định kỳ thống kê kết quả giám sát, tình hình cảnh báo và xử lý tấn công, rủi ro, sự cố an toàn thông tin.

- Báo cáo tổng hợp thống kê về tình hình giám sát an toàn thông tin: Lập báo cáo tổng hợp công tác giám sát an toàn thông tin định kỳ; Phiếu trình/ tờ trình, lãnh đạo xem xét kết quả báo cáo; Chỉnh sửa báo cáo theo ý kiến chỉ đạo, phê duyệt báo cáo và gửi báo cáo cho cơ quản chủ quản hệ thống.

b) Định mức

Đơn vị tính: Ngày

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
HNI.05.06.01	*Nhân công*		
	Kỹ sư bậc 2	Công	0,542
	Kỹ sư bậc 3	Công	2,167
	Kỹ sư bậc 4	Công	1,740
	Vật liệu		
	Giấy A4	Ram	0,022
	Bút	Cái	0,042
	Mực in	Hộp	0,011
	Máy, thiết bị		
	Máy tính	Ca	2,167
	Máy tính xách tay	Ca	2,281
	Máy chủ	Ca	0,604
	Hệ thống phục vụ phòng, chống xâm nhập lớp mạng	Ca	0,604
	Hệ thống phục vụ phòng chống mã độc	Ca	0,604
	Hệ thống phục vụ phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối	Ca	0,604
	Máy in	Ca	0,013

HNI.05.06.02. Giám sát gián tiếp

a) Thành phần công việc:

- Tiếp nhận thông tin giám sát.
    - Thu thập thông tin từ các nguồn.
    - Kiểm tra, rà soát đối tượng cần giám sát.
- Tổng hợp, phân loại thông tin, dữ liệu thu thập được.
    - Thu thập, phân loại thông tin dựa trên kết quả rà quét định kỳ.
    - Nghiên cứu kết quả phân tích thông tin.
    - Tổng hợp thông tin thu thập được sau kiểm tra, rà soát, rà quét định kỳ các đối tượng giám sát.
- Kiểm tra, phân tích chứng cứ, dữ liệu để phát hiện bất thường.
- Điều tra, xác minh nhằm xác định nguy cơ, sự cố xảy ra với đối tượng giám sát.
    - Nghiên cứu điều tra, xác minh, xác định nguy cơ, sự cố xảy ra đối với đối tượng giám sát.
    - Trao đổi thông tin với đối tượng chủ quản của hệ thống được giám sát.
- Đánh giá nguy cơ mất an toàn thông tin hoặc sự cố.
    - Nghiên cứu dữ liệu đã phân tích và thông tin xác nhận từ đơn vị, cá nhân chủ quản/sử dụng hệ thống thông tin.
    - Thực hiện đánh giá nguy cơ mất an toàn thông tin hay sự cố an toàn thông tin của hệ thống thông tin, đánh giá mức độ ảnh hưởng của sự cố lên hệ thống thông tin.
- Phân tích chuyên sâu, phân loại rủi ro, sự cố an toàn thông tin.
    - Phân tích chuyên sâu để xác định phương thức, thủ đoạn, cách thức tấn công, nguồn tấn công, mục tiêu tấn công, mục đích tấn công.
    - Thực nghiệm trong môi trường giả lập để xác định phương thức, thủ đoạn, cách thức tấn công, nguồn tấn công, mục tiêu tấn công, mục đích tấn công
    - Thực nghiệm trực tiếp trên hệ thống thông tin được giám sát để xác định phương thức, cách thức tấn công; xác định mục tiêu, mục đích tấn công.
    - Đánh giá mức độ nghiêm trọng, thiệt hại.
- Thực hiện cảnh báo với đơn vị, cá nhân chủ quản hệ thống thông tin: Thực hiện cảnh báo nguy cơ mất an toàn thông tin/sự cố an toàn thông tin với đơn vị, cá nhân chủ quản/sử dụng hệ thống thông tin và lập báo cáo cảnh báo.
- Xem xét, đề xuất phương án xử lý, xin chỉ thị cấp trên: Nghiên cứu, đề xuất phương án xử lý nguy cơ/sự cố an toàn thông tin và báo cáo lãnh đạo và xin chỉ thị trong trường hợp đơn vị, cá nhân chủ quản/sử dụng hệ thống thông tin không

xử lý được nguy cơ mất an toàn thông tin hoặc sự cố an toàn thông tin và có yêu cầu nhờ hỗ trợ xử lý và Báo cáo xin chỉ thị của lãnh đạo cấp trên.

- Xử lý nguy cơ, sự cố xảy ra với đối tượng giám sát: Thiết lập biện pháp kỹ thuật xử lý các nguy cơ/ sự cố xảy ra với đối tượng giám sát.

  - Thiết lập các biện pháp kỹ thuật xử lý nguy cơ/sự cố phần mềm.
  - Thiết lập các biện pháp kỹ thuật xử lý nguy cơ/sự cố thiết bị.

- Tiếp tục theo dõi nhằm xác định nguy cơ, sự cố xảy ra với đối tượng giám sát: Triển khai theo dõi nguy cơ mất an toàn thông tin hoặc sự cố an toàn thông tin đã được xử lý nhằm đảm bảo nguy cơ, sự cố đã được xử lý triệt để trên hệ thống thông tin được giám sát; Thu thập thông tin; Theo dõi, giám sát các sự cố tái phát sinh hoặc diễn biến mới; Đề xuất phương án xử lý.

- Cập nhật, điều chỉnh hệ thống giám sát định kỳ.

  - Thu thập thông tin về các lỗ hổng bảo mật, mã độc được công bố, các phương thức tấn công mạng mới…; Nghiên cứu, cập nhật các diễn biến mới về tình hình an toàn thông tin trong nước và quốc tế. Phân loại, phân tích các lỗ hổng bảo mật, mã độc, các phương thức tấn công mạng mới và đưa ra nhận định mức độ ảnh hưởng đối hệ thống thông tin đang được giám sát.
  - Viết tệp luật nhằm nhận diện lỗ hổng bảo mật, các phương thức tấn công mạng mới; Thử nghiệm tệp luật trên hệ môi trường giả lập; Cập nhật tệp luật cho toàn bộ thiết bị quan trắc; Tối ưu hệ thống.

- Định kỳ thống kê kết quả giám sát, tình hình cảnh báo và xử lý tấn công, rủi ro, sự cố an toàn thông tin.

- Báo cáo tổng hợp thống kê về tình hình giám sát an toàn thông tin: Lập báo cáo tổng hợp công tác giám sát an toàn thông tin định kỳ; Phiếu trình/tờ trình, lãnh đạo xem xét kết quả báo cáo; Chỉnh sửa báo cáo theo ý kiến chỉ đạo, phê duyệt báo cáo và gửi báo cáo cho cơ quản chủ quản hệ thống.

b) Định mức

Đơn vị tính: Ngày

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
HNI.05.06.02	*Nhân công*		
	Kỹ sư bậc 2	Công	0,479
	Kỹ sư bậc 3	Công	1,000
	Kỹ sư bậc 4	Công	1,073
	Vật liệu		
	Giấy A4	Ram	0,022

	Bút	Cái	0,042
	Mực in	Hộp	0,011
	Máy, thiết bị		
	Máy tính	Ca	1,167
	Máy tính xách tay	Ca	1,385
	Máy chủ	Ca	0,625
	Hệ thống thu thập, phân tích dữ liệu	Ca	0,625
	Máy in	Ca	0,013

HNI.05.07.00. Rà quét, xử lý mã độc cho các cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội trên địa bàn thành phố

a) Thành phần công việc

- Thu thập, phân tích thông tin ứng dụng có kết nối, hoạt động bất thường trên hệ thống.
  - Phân tích dữ liệu về lưu lượng kết nối.
  - Phân tích dữ liệu về các địa chỉ thực hiện rà quét trên hệ thống.
- Sao lưu hệ thống trước và sau khi xử lý sự cố.
- Tiêu diệt các mã độc, phần mềm độc hại.
- Khôi phục hệ thống, dữ liệu và kết nối.
- Cấu hình hệ thống an toàn; Khắc phục các điểm yếu an toàn thông tin.
- Kiểm tra thử toàn bộ hệ thống sau khi khắc phục sự cố.
- Đề xuất bổ sung các thiết bị, phần cứng, phần mềm bảo đảm an toàn thông tin cho hệ thống.
- Xây dựng báo cáo đánh giá.
- Lưu hồ sơ công việc.

b) Định mức

Đơn vị tính: Hệ thống

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
HNI.05.07.00	*Nhân công*		
	Kỹ sư bậc 3	Công	0,417
	Kỹ sư bậc 4	Công	0,354
	Vật liệu		
	Giấy A4	Ram	0,040
	Bút	Cái	0,040
	Mực in	Hộp	0,020

	Máy, thiết bị		
	Máy tính	Ca	0,250
	Máy tính xách tay	Ca	0,521
	Hệ thống rà quét mã độc	Ca	0,177
	Máy in	Ca	0,010

HNI.05.08.00. Giám sát phòng, chống, ngăn chặn thư rác, tin nhắn rác cho các cơ quan Đảng, Nhà nước, tổ chức chính trị-xã hội trên địa bàn thành phố

a) Thành phần công việc

- Thu thập thông tin thư rác trên hệ thống.
- Đánh giá, phân loại thư rác.
- Kiểm tra thông tin địa chỉ thư rác gửi đến.
- Cài đặt, cấu hình hệ thống phòng, chống, ngăn chặn thư rác.
- Thực hiện đưa các địa chỉ rác vào blacklist.
- Gỡ bỏ MxToolbox Blacklist Summary.
- Hướng dẫn sử dụng.
- Tổng hợp, lập báo cáo.

b) Định mức

Đơn vị tính: Ngày

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
HNI.05.08.00	*Nhân công*		
	Kỹ sư bậc 3	Công	0,521
	Kỹ sư bậc 4	Công	0,271
	Vật liệu		
	Giấy A4	Ram	0,040
	Bút	Cái	0,040
	Mực in	Hộp	0,020
	Máy, thiết bị		
	Máy tính	Ca	0,792
	Máy in	Ca	0,010

HNI.05.09.00. Ứng cứu, xử lý sự cố tấn công thay đổi giao diện, lỗ hổng bảo mật phần mềm ứng dụng

HNI.05.09.01. Sự cố thông thường

a) Thành phần công việc

- Tiếp nhận thông tin sự cố qua các công cụ giám sát hoặc qua cảnh báo.

- Phân loại, đánh giá sự cố về tình trạng, mức độ sự cố.
- Triển khai ứng cứu sự cố:
  - Tạm dừng hoạt động của phần mềm ứng dụng trên internet và ra thông báo gửi đơn vị trong quá trình xử lý sự cố.
  - Gỡ bỏ các nội dung thay đổi, xuyên tạc trên giao diện phần mềm ứng dụng.
  - Kiểm tra, xử lý lỗ hổng bảo mật, mã độc.
- Khôi phục lại dữ liệu của phần mềm ứng dụng thời điểm trước khi bị tấn công.
- Kiểm tra kết quả khắc phục sự cố.
- Đưa phần mềm ứng dụng trở lại hoạt động bình thường trên môi trường Internet.
- Tổng hợp, lập báo cáo.

b) Định mức

Đơn vị tính: Sự cố

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
HNI.05.09.01	*Nhân công*		
	Kỹ sư bậc 3	Công	1,290
	Kỹ sư bậc 4	Công	1,073
	Kỹ sư bậc 5	Công	1,000
	Vật liệu		
	Giấy A4	Ram	0,040
	Bút	Cái	0,040
	Mực in	Hộp	0,020
	Máy, thiết bị		
	Máy tính	Ca	0,115
	Máy tính xách tay	Ca	3,248
	Máy in	Ca	0,010

HNI.05.09.02. Sự cố phức tạp

a) Thành phần công việc

- Phát hiện, tiếp nhận thông tin sự cố.
- Xác minh, phân tích, đánh giá và phân loại sự cố
- Xác định và lựa chọn phương án ứng cứu.
- Triển khai ứng cứu sự cố:

- Tạm dừng hoạt động của phần mềm ứng dụng trên internet và ra thông báo gửi đơn vị trong quá trình xử lý sự cố.
- Gỡ bỏ các nội dung thay đổi, xuyên tạc trên giao diện phần mềm ứng dụng.
- Kiểm tra, xử lý lỗ hổng bảo mật, mã độc.

- Tiến hành các biện pháp khôi phục tạm thời.

- Ngăn chặn, xử lý hậu quả.

- Kiểm tra kết quả khắc phục sự cố.

- Đưa phần mềm ứng dụng trở lại hoạt động bình thường trên môi trường Internet.

- Tổng hợp, lập báo cáo.

b) Định mức

Đơn vị tính: Sự cố

Mã định mức	Thành phần hao phí	Đơn vị tính	Hao phí
HNI.05.09.02	*Nhân công*		
	Kỹ sư bậc 3	Công	1,425
	Kỹ sư bậc 4	Công	1,769
	Kỹ sư bậc 5	Công	1,813
	Vật liệu		
	Giấy A4	Ram	0,040
	Bút	Cái	0,040
	Mực in	Hộp	0,020
	Máy, thiết bị		
	Máy tính	Ca	0,115
	Máy tính xách tay	Ca	4,892
	Máy in	Ca	0,010