

PHỤ LỤC 1:
CÁC HẠNG MỤC CÔNG VIỆC THỰC HIỆN
XÁC ĐỊNH CẤP ĐỘ 2 THEO NGHỊ ĐỊNH 85/2016/NĐ-CP

TT	Công đoạn	Công việc thực hiện
1	Khảo sát hiện trạng sơ bộ	Xác định phạm vi triển khai, tiêu chuẩn tham chiếu. - Xác định chủ quản hệ thống thông tin. - Xác định đơn vị vận hành hệ thống thông tin. - Xác định đơn vị vận hành, quản trị ứng dụng của hệ thống thông tin. - Xác định các đối tác nhà cung cấp có liên quan.
2	Khảo sát chi tiết	Khảo sát chi tiết mô hình kiến trúc mạng, các giải pháp triển khai. Bao gồm các hạng mục: 1. Bảo đảm an toàn mạng (thiết kế, giải pháp An toàn thông tin áp dụng) 2. Bảo đảm an toàn máy chủ. 3. Bảo đảm an toàn ứng dụng. 4. Bảo đảm an toàn dữ liệu. Khảo sát chi tiết các chính sách An toàn thông tin của Đơn vị: Theo các phạm vi yêu cầu sau: Chính sách An toàn thông tin. (Quản lý an toàn mạng, Quản lý an toàn máy chủ và ứng dụng, Quản lý an toàn dữ liệu; Quản lý an toàn thiết bị đầu cuối; Quản lý phòng chống phần mềm độc hại; Quản lý điểm yếu ATTT; Quản lý giám sát ATHTTT; Quản lý an toàn sử dụng đầu cuối, công bố và rà soát sửa đổi). 1. Tổ chức đảm bảo An toàn thông tin. 2. An toàn nguồn nhân lực. 3. An toàn trong thiết kế và xây dựng hệ thống. 4. An toàn trong vận hành hệ thống. 5. Quản lý rủi ro An toàn thông tin. 6. Phương án kết thúc vận hành, khai thác, thanh lý và hủy bỏ.
3	Phân tích đánh giá	Đánh giá các chính sách ATTT còn thiếu so với yêu cầu của quy định Đánh giá kiến trúc mạng và các giải pháp An toàn thông tin còn thiếu so với yêu cầu.
4	Xây dựng hồ sơ cấp độ	Xây dựng hồ sơ cấp độ và thực hiện thủ tục phê duyệt. 1. Thuyết minh tổng quan về hệ thống thông tin. 2. Thuyết minh cấp độ đề xuất 3. Thuyết minh phương án đảm bảo an toàn thông tin. 3.1 Thuyết minh đáp ứng yêu cầu về chính sách ATTT đã được xây dựng và ban hành. 3.2 Thuyết minh đáp ứng yêu cầu về giải pháp đã được triển khai.

5	Hướng dẫn xây dựng các Quy trình liên quan theo các quy định hiện hành	Xây dựng biểu mẫu, khung các quy trình: 1. Quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi thôi việc 2. Quy trình thử nghiệm và nghiệm thu hệ thống 3. Quy trình quản lý an toàn mạng 4. Quy trình quản lý an toàn máy chủ và ứng dụng 5. Quy trình quản lý an toàn dữ liệu 6. Quy trình quản lý sự cố an toàn thông tin 7. Quy trình quản lý an toàn người sử dụng đầu cuối 8. Quy trình về quản lý rủi ro an toàn thông tin 9. Quy trình kết thúc vận hành, khai thác, thanh lý, hủy bỏ
6	Xây dựng Báo cáo Hiện trạng và Kế hoạch hành động	1. Trình bày chi tiết các điểm yếu, rủi ro và sự thiếu tuân thủ đã được phát hiện. 2. Danh mục các chính sách, quy trình cần xây dựng mới hoặc cập nhật để đáp ứng quy định. 3. Phân chia các giải pháp thành các giai đoạn (ngắn hạn, trung hạn, dài hạn). 4. Sắp xếp thứ tự ưu tiên dựa trên mức độ rủi ro, yêu cầu tuân thủ và nguồn lực của đơn vị. 5. Cung cấp ước tính sơ bộ về chi phí đầu tư và nhân lực thực hiện để ban lãnh đạo có cơ sở lập ngân sách.