QUY ĐỊNH VỀ AN TOÀN VÀ BẢO MẬT DỮ LIỆU ĐIỆN TỬ

1. An toàn và bảo mật hệ thống (HT mạng, máy chủ)

1.1. Quản lý an toàn và bảo mật phòng máy chủ

- IT quản trị hệ thống có trách nhiệm quản lý phòng máy chủ, phòng máy chủ luôn phải khóa khi không có người. Người không có phận sự không được ra vào phòng máy chủ.
- Chỉ nhân viên IT của công ty được phân công công việc liên quan mới được phép truy cập vào hệ thống. Những trường hợp khác phải được sự đồng ý của cán bộ phụ trách bộ phận IT và phải có sự giám sát của nhân viên IT.
- Nhân viên IT có nhu cầu làm việc ngoài giờ tại phòng máy chủ phải được sự đồng ý của cán bộ phụ trách IT.
- Các máy móc, thiết bị liên quan đến lưu trữ dữ liệu khi mang vào và mang ra khỏi phòng máy chủ phải được sự đồng ý của cán bộ quản lý bộ phận IT và phải ghi chép vào Sổ nhật ký theo dõi phòng máy chủ (BM01/14). Khi mang MMTB ra ngoài công ty thực hiện theo quy định tại QT63/TH.
- Các công việc bảo trì, sửa chữa, xử lý sự cố liên quan đến máy chủ phải ghi vào Sổ nhật ký theo dõi phòng máy chủ (BM01/14).

1.2.Biện pháp kỹ thuật đảm bảo an toàn hệ thống:

- Đảm bảo hoạt động ổn định của máy chủ bằng việc: Duy trì nguồn điện để máy chủ hoạt động liên tục 24/7, thực hiện bảo trì định kỳ để tăng tuổi thọ máy và phòng ngừa các sự cố.
- Bảo mật hệ thống mạng và truyền tin: Hệ thống mạng và đường truyền phải áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp như sử dụng tường lửa (Firewall) và phải thường xuyên theo dõi phát hiện kịp thời các hoạt động xâm nhập và có biện pháp xử lý kịp thời.
- Quản lý hệ thống mạng nội bộ: Mạng nội bộ của công ty phải được tổ chức theo mô hình Clients/Server; mạng nội bộ khi kết nối với mạng Internet phải thông qua thiết bị tường lửa kiểm soát, có phân chia hệ thống mạng nội bộ thành các vùng mạng theo phạm vi truy cập, vô hiệu hóa tất cả các dịch vụ không sử dụng tại từng vùng mạng, thực hiện nguyên tắc chỉ mở các dịch vụ cần thiết khi có yêu cầu.

- Quản lý hệ thống mạng không dây (wifi): Khi thiết lập mạng không dây có kết nối vào mạng nội bộ phải thiết lập các thông số cần thiết như định danh, mật mã, mã hóa dữ liệu.
- Quản lý truy cập từ xa vào mạng nội bộ: Cá nhân có nhu cầu truy cập từ xa vào mạng nội bộ, phần mềm của công ty (trừ PM QLVB) phải có đề nghị được Giám đốc duyệt. Đối với việc truy cập từ xa vào mạng nội bộ bắt buộc phải sử dụng VPN (mạng riêng ảo) và phải được theo dõi, quản lý chặt chẽ, phải thiết lập mật mã độ an toàn cao, thường xuyên thay đổi mật mã, không truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng.

2. An toàn, bảo mật dữ liệu điện tử

2.1. Kiểm soát dữ liệu và thông tin trên máy tính

2.1.1. Quy định chung

- Máy tính (Bao gồm các máy tính lưu trữ tài liệu hệ thống, máy tính kết nối thiết bị phân tích) phải đặt mật khẩu khi đăng nhập và được phân quyền. Khi không làm việc với máy vi tính trong thời gian từ 30 phút trở lên, CBCNV phải tắt máy tính hoặc đặt chế độ bảo vệ để đảm bảo an toàn cho dữ liệu của cá nhân.
- Khi được cấp tài khoản sử dụng phần mềm (thường kèm theo tên đăng nhập và mật khẩu mặc định), cần thay đổi mật khẩu trước khi sử dụng và có trách nhiệm bảo mật tài khoản truy cập được cấp. Mỗi tài khoản sử dụng phải có cá nhân chịu trách nhiệm quản lý tài khoản.
- Nguyên tắc đặt mật khẩu phải có độ phức tạp (thường có độ dài từ 6-8 ký tự bao gồm cả chữ thường, chữ hoa, số, ký tự đặc biệt như @, #, &,...).
- Trong trao đổi thông tin, dữ liệu phục vụ công việc, CBCNV phải sử dụng hệ thống thông tin của công ty như Phần mềm quản lý văn bản, email công ty. Không sử dụng các phương tiện email khác, mạng xã hội,... để gửi file dữ liệu của công ty.
- Nghiêm cấm sử dụng các thiết bị lưu trữ bên ngoài như USB, HDD box,... để copy dữ liệu của công ty.
- Phòng, chống virus: Cán bộ, công nhân viên có trách nhiệm tuân thủ các biện pháp phòng và chống virus cho máy tính, đảm bảo an toàn dữ liệu thuộc cá nhân quản lý. Khi máy tính có hiện tượng nhiễm virus, người dùng phải báo ngay cho IT để tách máy tính khỏi hệ thống mạng chung tránh tình trạng lây nhiễm sang các máy tính khác sau đó sẽ xử lý bằng các biện pháp kỹ thuật của IT. Không truy cập vào các link liên kết không rõ ràng; không vào các đường link hoặc tải về các file tài liệu từ các địa chỉ không rõ thông tin, nguồn gốc của người gửi.

2.1.2. Đối với các máy tính có kết nối với thiết bị phân tích

- Quy định mật khẩu: Như mục Quy định chung 2.1.1
- Các cổng kết nối: Phải được khóa nhằm ngăn chặn việc sao chép dữ liệu
- Thời gian hiệu lực của mật khẩu là: 90 ngày
- Người được phân công tạo các thư mục để chứa các dữ liệu phân tích theo từng tháng cho từng KNV và KNV lưu theo đường dẫn quy định như sau:

  Computer/ổ..... /Năm...../ Mã TBi ...../ Tên KNV

2.2. Kiểm soát phần mềm thiết bị phân tích

- Mỗi KNV được cấp ít nhất 1 user để sử dụng phần mềm
- Mật khẩu truy cập phần mềm: Gồm 4-8 ký tự và 4-6 số
- Thời gian có hiệu lực của mật khẩu là: 30 ngày
- Việc đăng nhập sẽ bị khóa sau: 30 phút
- Phân quyền sử dụng phần mềm theo SOP17/07
- Khi KNV không còn sử dụng tài khoản thì admin sẽ xóa tài khoản đó.

2.3. Sao lưu dữ liệu

2.3.1. Các dữ liệu lưu trữ trên máy chủ

- Gồm: Dữ liệu ERP, nhân sự, chấm công, dữ liệu các bộ phận sao lưu lên ổ Z (File Server).
- IT đặt chế độ sao lưu dữ liệu tự động 1 lần/ngày.

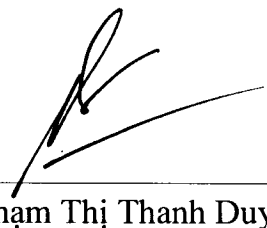
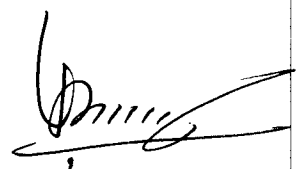
2.3.2. Dữ liệu của bộ phận QC

- Bao gồm toàn bộ các dữ liệu phân tích, ảnh sắc ký lớp mỏng, các dữ liệu gốc của các thiết bị như nồi hấp, tủ bảo quản CĐC...

+ Đối với các dữ liệu không kết nối trực tiếp với máy tính nhưng có thể trích xuất dữ liệu: Người được phân công phụ trách phải sao lưu định kỳ dữ liệu điện tử ít nhất 1 lần/tháng vào ngày cuối cùng của tháng. Cách thức: Sao lưu toàn bộ dữ liệu cần thiết trong kỳ vào đường dẫn: K:\1.DATA PHAN TICH\NAM...\MATHIETBI...\TEN DU LIEU...\THANG...

+ Đối với các thiết bị có kết nối mạng nội bộ: Như HPLC, UV-VIS, IR...: Thực hiện sao lưu định kỳ ít nhất 1 lần/tháng vào ngày cuối cùng của tháng. Sao lưu vào đường dẫn: K:\1.DATA PHAN TICH\NAM...\MATHIETBI...\THANG...

+ Quá trình sao lưu dữ liệu do 01 cán bộ được Trưởng phòng QLCL phân công thực hiện và phải được ghi chép lại vào BM17/67. Các dữ liệu sau khi đã sao lưu lên thiết bị lưu trữ, IT đặt lại quyền chỉ đọc (không sửa, xóa) của thư mục đó cho Trưởng phòng QLCL truy cập vào xem.

	Người phê duyệt	**Người soát xét**	**Người soạn thảo**
Ngày	08/06/2023	08/06/2023	08/06/2023
Ký tên			
Họ tên	Phạm Thị Thanh Duyên	Hoàng Thị Hường	Nguyễn Thị Thanh Nga