

Quy định về bảo mật thông tin

Ver 1.1

Nội dung:

1. Quy định chung phòng tránh rò rỉ thông tin
2. Quy định vào/ ra công ty
3. Quy định về sử dụng máy tính
4. Quy định về sử dụng Email/ ChatWork
5. Xử lý khi gặp sự cố bảo mật thông tin
6. Cơ cấu quản lý bảo mật thông tin

- Về nguyên tắc, không được mang tài liệu của công ty, tài liệu phát triển dự án... ra ngoài.
- Trong trường hợp cần mang/gửi tài liệu ra ngoài vì mục đích công việc thì phải xin xác nhận của người phụ trách bảo mật.
- Trong trường hợp lưu tài liệu trên USB, Laptop mang ra ngoài thì phải áp dụng các biện pháp bảo mật, mã hóa thiết bị.
- Chỉ được sử dụng USB/ Laptop do công ty cung cấp. Tuyệt đối không đem theo/ sử dụng USB cá nhân, máy tính cá nhân ở văn phòng công ty dưới mọi hình thức.
- Không được quay phim, chụp ảnh, video call... trong công ty, trong trường hợp cần thiết cho công việc phải xin xác nhận của người phụ trách bảo mật.
- Hàng ngày trước khi về dọn bàn làm việc sạch sẽ, không được để tài liệu, thiết bị test... trên bàn.

- Đảm bảo cửa vào/ra văn phòng luôn đóng, quản lý vào ra bằng vân tay.
- Hàng ngày, nhân viên rời công ty cuối cùng phải kiểm tra đầy đủ các hạng mục quy định và ký xác nhận vào checksheet.
- Khi có khách đến công ty, người phụ trách phải phổ biến quy định bảo mật thông tin đầy đủ (cấm quay phim, chụp ảnh ...).
- Trong trường hợp có nhân viên nhà thầu đến sửa chữa, lắp đặt... thì phải có người giám sát.

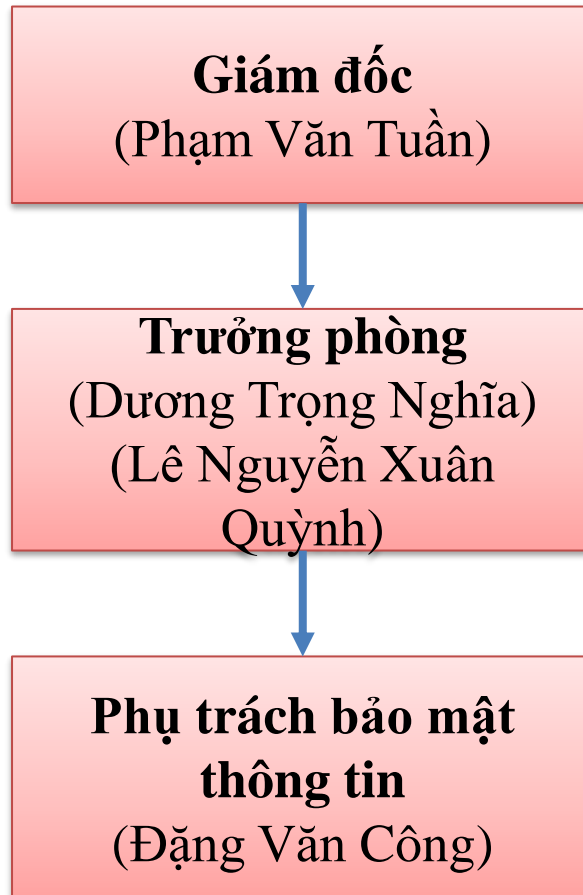
3. Quy định về sử dụng máy tính

- Luôn luôn khóa màn hình (window + L) khi rời khỏi chỗ ngồi.
- Thiết lập tự động khóa màn hình (screen save) sau tối đa 10 phút.
- Tuyệt đối không kết nối các thiết bị cá nhân với máy tính công ty (cắm sạc điện thoại, USB...).
- Tuyệt đối không tự ý cài thêm phần mềm vào máy tính, trong trường hợp cần thiết phải xin xác nhận của người phụ trách bảo mật.
- Để laptop vào tủ có khóa sau giờ làm việc hoặc khi không sử dụng trong thời gian dài.

4. Quy định về sử dụng Email/ ChatWork/GitHub

- Không gửi tài liệu, file đính kèm qua Email/ChatWork. Trong trường hợp cần thiết phục vụ công việc thì phải xin xác nhận của bộ phận và phải mã hóa, đặt mật khẩu bảo mật. Không gửi mật khẩu cùng file đính kèm trong cùng một mail.
- Trong nội bộ công ty chỉ được chia sẻ qua server, tuyệt đối không gửi qua mail, chatwork...
- Khi nhận được email, link, file không rõ nguồn gốc tuyệt đối không mở email, truy cập link, file và phải báo ngay với người phụ trách bảo mật.

- Khi có nguy cơ hoặc xảy ra bất kỳ sự cố liên quan đến bảo mật thông tin phải báo ngay với người phụ trách bảo mật. Trong trường hợp nghi ngờ máy nhiễm virus, malware, phải ngắt kết nối internet ngay lập tức.



Số điện thoại liên lạc khẩn cấp:

Phạm Văn Tuấn : 094-3455-215

Dương Trọng Nghĩa: 097-5868-872

Lê Nguyễn Xuân Quỳnh:

Đặng Văn Công: