



THÔNG TIN KHAI GIẢNG

Thời lượng : 2 ngày

Giờ học : 8h/ngày

Hình thức : Trực tiếp

Public

E-Learning



GỬI TRỌN NIỀM TIN

BLT.cert

LIÊN HỆ CHÚNG TÔI

VPGD Miền Bắc: số 23 ngách 37/2 Ngõ 37 phố Dịch Vọng, Q. Cầu Giấy, TP. Hà Nội

VPGD Miền Nam: 138 Lê Văn Sỹ, Phường 10, Phú Nhuận, Thành phố Hồ Chí Minh.

0916 757 881

contact@bltcert.vn

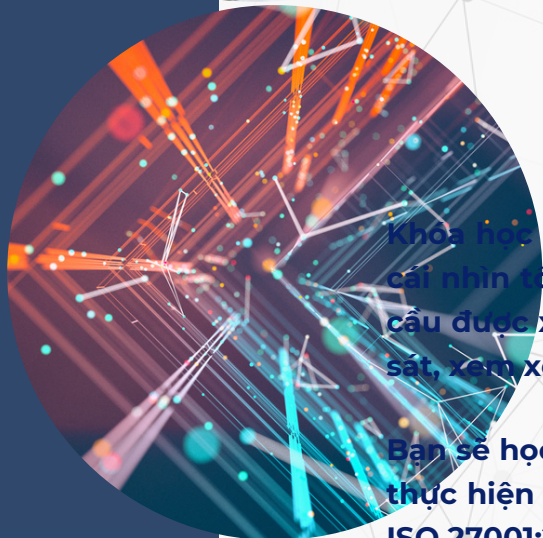
www.bltcert.vn

KHÓA ĐÀO TẠO

NHẬN THỨC VỀ HỆ THỐNG QUẢN LÝ

AN TOÀN THÔNG TIN

ISO 27001:2013



GIỚI THIỆU

Khóa học này do các chuyên gia bảo mật thông tin của chúng tôi cung cấp và nhằm cung cấp cho bạn cái nhìn tổng quan về lợi ích và mục đích của hệ thống quản lý an ninh thông tin (HTQL ATTT). Các yêu cầu được xem xét chi tiết, cùng với các quá trình liên quan đến việc thiết lập, thực hiện, vận hành, giám sát, xem xét và cải tiến hệ thống HTQL ATTT.

Bạn sẽ học cách bảo vệ tổ chức của mình khỏi vi phạm bảo mật thông tin và hiểu những lợi thế của việc thực hiện các yêu cầu của ISO 27001:2013 và đạt được chứng chỉ tham dự Khóa đào tạo các yêu cầu của ISO 27001:2013 của BLT.cert.

ĐỐI TƯỢNG THAM DỰ

Các cá nhân làm việc cho bất kỳ lĩnh vực kinh doanh nào có tương tác với dữ liệu và thông tin của các bên liên quan như quản lý và bảo vệ dữ liệu, dịch vụ CNTT, nguồn nhân lực và tài chính & kế toán...

- Quản lý bảo mật thông tin.
- Quản lý CNTT và bảo mật doanh nghiệp.
- Giám đốc quản trị công ty.
- Người quản lý rủi ro và tuân thủ.
- Tư vấn bảo mật thông tin.



MỤC TIÊU

✓ Tổ chức của bạn sẽ có một nguồn lực nội bộ và quy trình để lập kế hoạch và thiết lập một HTQL ATTT.

✓ Nâng cao kiến thức của bạn về HTQL ATTT.

✓ Hỗ trợ tổ chức bảo vệ dữ liệu nhạy cảm, tức là dữ liệu cá nhân, bí mật kinh doanh, tuân thủ các yêu cầu pháp lý, luật pháp và quản trị.

✓ Hiểu được khoảng cách giữa HTQL ATTT hiện tại và các tiêu chuẩn quốc tế.



ĐĂNG KÝ NGAY

NỘI DUNG ĐÀO TẠO

- › Lợi ích, mục đích và các quy trình liên quan đến quản lý HTQL ATTT.
- › Mục đích, mục đích và hiểu biết về các yêu cầu đối với chứng nhận ISO 27001.
- › Các nguyên tắc cơ bản của tiêu chuẩn và tổng quan về chu trình (PDCA).
- › Cách tiếp cận cơ bản để đánh giá rủi ro.
- › Phát triển cơ sở hạ tầng an toàn thông tin.
- › Để xác định tài sản, chủ sở hữu rủi ro, mối đe dọa, lỗ hổng bảo mật và tác động kinh doanh.
- › Để xác định bất kỳ khoảng trống nào trong các kiểm soát hiện có của bạn và giải quyết các kiểm soát trong Phụ lục A của tiêu chuẩn.
- › Các đối tượng của tính bảo mật, tính toàn vẹn và tính sẵn có của thông tin và tầm quan trọng của những thông tin này khi đánh giá rủi ro và thực hiện các biện pháp kiểm soát.
- › Thiết kế, triển khai và xem xét phương pháp luận đánh giá rủi ro.

