Nguyên lý 1: Không có an toàn tuyệt đối

Nguyên lý 2: Ba mục tiêu bảo mật là tính bảo mật, tính toàn vẹn và tính khả dụng

Nguyên lý 3: Phòng thủ theo chiều sâu

Nguyên lý 4: Khả năng chấp nhận tâm lý

Nguyên lý 5: Bảo mật máy tính phụ thuộc vào hai loại yêu cầu: Chức năng và Đảm bảo

Nguyên lý 6: Bảo mật thông qua sự che giấu là sai

Nguyên lý 7: An ninh bằng với quản lý rủi ro

Nguyên lý 8: Ba loại kiểm soát an ninh là Phòng ngừa, Thám tử và Phản ứng

Nguyên lý 9: Đơn giản trong sử dụng

Nguyên lý 10: Sợ hãi, không chắc chắn và nghi ngờ không có tác dụng bán an ninh

Nguyên lý 11: Tất cả con người, quy trình và công nghệ đều cần thiết để đảm bảo đầy đủ cho một hệ thống hoặc cơ sở

Nguyên lý 12: Thiết kế mở trong đảm bảo an toàn thông tin

Nguyên lý 13: Phân quyền

Nguyên lý 14: Đặc quyền tối thiểu

Nguyên lý 15: Mặc định an toàn

Nguyên lý 16: Toàn diện

Nguyên lý 17: Phổ biến tối thiểu

Nguyên lý 18: Cách ly trong đảm bảo an toàn thông tin

Nguyên lý 19: Đóng gói trong đảm bảo an toàn thông tin

Nguyên lý 20: Mềm dẻo hệ thống

Nguyên lý 21: Tường minh trong đảm bảo an toàn thông tin

Nguyên lý 22: Tính hệ thống

Nguyên lý 23: Đảm bảo an toàn thông tin tổng thể

Nguyên lý 24: Đảm bảo an toàn thông tin liên tục

Nguyên lý 25: Ghi âm thỏa hiệp

Nguyên lý 26: Yếu tố công việc

Triển khai bảo mật phân lớp (Đảm bảo không có điểm dễ bị tấn công)

Tách hệ thống truy cập công cộng khỏi các tài nguyên quan trọng của sứ mệnh.

Thực hiện bảo mật thông qua sự kết hợp của các biện pháp được phân phối vật lý và logic.

Use unique identities to ensure accountability.