Đào tạo nhận thức
An toàn thông tin

GEM
YOUR TRUSTED PARTNER

Theo tiêu chuẩn ISO/IEC 27001:2013

GEM July 2023

CONFIDENTIAL

Nội dung đào tạo

GEM
YOUR TRUSTED PARTNER

01 Thông tin và An toàn thông tin

02 Các rủi ro ATTT phổ biến

03 Hậu quả từ các sự cố ATTT

04 Hệ thống quản lý ATTT (ISMS)

05 Chính sách, quy định ATTT phải tuân thủ

CONFIDENTIAL

01

Thông tin và An toàn thông tin

CONFIDENTIAL

Các dạng tồn tại của thông tin

Từng giây từng phút chúng ta đề tiếp xúc với thông tin ở các dạng tồn tại khác nhau:

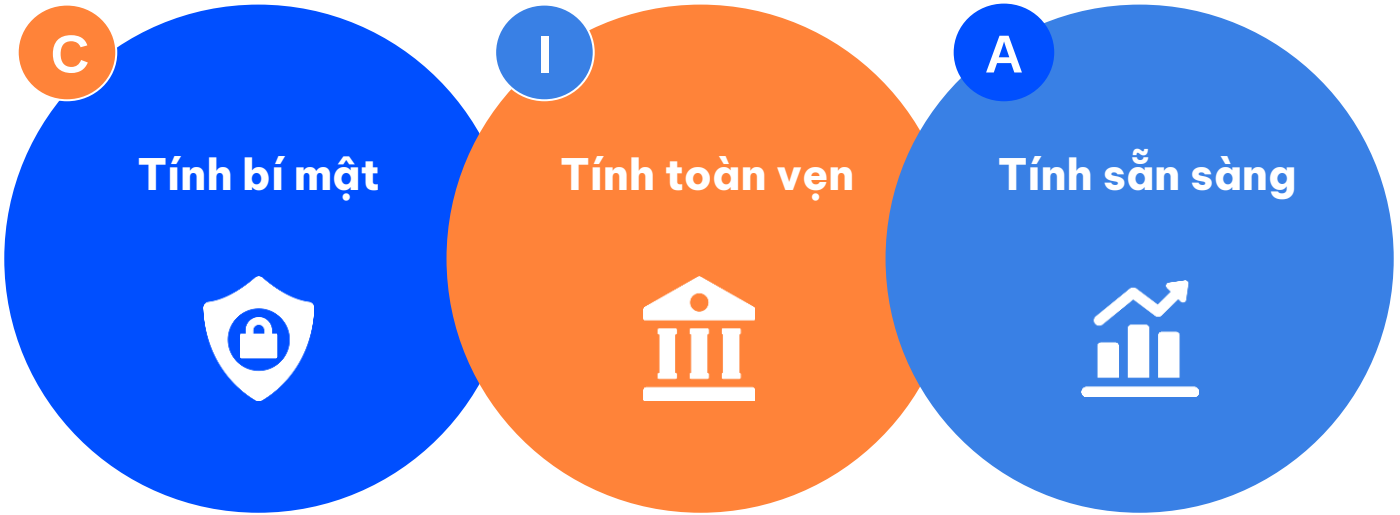
Thông tin là gì

- Thông tin là một loại tài sản
- Giống như tất cả các tài sản kinh doanh khác của công ty
- Thông tin có giá trị quan trọng đối với Công ty nên phải được bảo vệ một cách thích hợp

- Theo ISO/IEC 27000:2018

An toàn thông tin là gì

Theo ISO/IEC 27000:2018, An toàn thông tin (ATTT) là bảo vệ ba tính chất trọng yếu của thông tin:



02

Các mối đe dọa và rủi ro ATTT phổ biến

CONFIDENTIAL

Tình hình ATTT tại Việt Nam năm 2022

Theo thống kê từ Viettel Threat Intelligence (Viettel Cyber Security - Threat Intelligence), năm 2022

- **150 triệu** thông tin tài khoản người dùng được rao bán trên không gian mạng
- **29 vụ** lộ lọt dữ liệu của các công ty phát triển phần mềm qua các nền tảng chia sẻ trực tuyến như Github
- **10 triệu** cuộc tấn công DDoS với cường độ tấn công >1G tăng dần theo từng quý
- **> 4.000** cuộc tấn công Phishing và Impersonate, giả mạo tin nhắn thương hiệu (SMS Brand name), tên miền phụ để truy cập

Một số loại mã độc phổ biến

GEM
YOUR TRUSTED PARTNER

Virus

Là những chương trình hay đoạn mã được thiết kế để tự nhân bản và sao chép chính nó tạo ra những tệp tin bị nhiễm virus

Trojan

Là chương trình độc hại ngụy trang như 1 phần mềm hoặc tệp an toàn

Phần mềm gián điệp

Là loại phần mềm chuyên thu thập trái phép các thông tin người dùng qua mạng Internet. Spyware thường được cài đặt bị mật kèm theo các phần mềm miễn phí

Phần mềm tống tiền

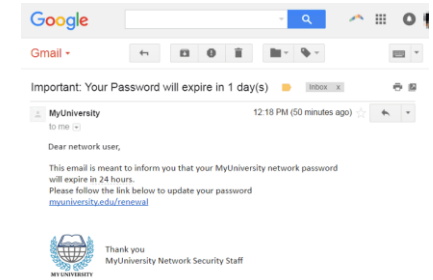
Là loại mã độc sử dụng một hệ thống mật mã để mã hóa dữ liệu thuộc về một cá nhân và đòi tiền chuộc thì mới khôi phục lại

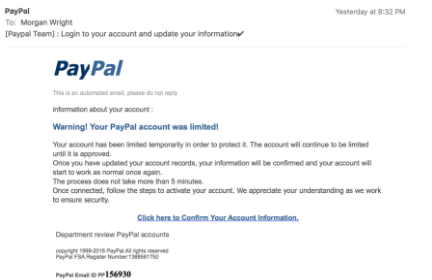
CONFIDENTIAL

Một số kiểu tấn công phổ biến

GEM
YOUR TRUSTED PARTNER

Phishing email





Ransomware

Adware

CONFIDENTIAL

Các rủi ro phổ biến

Thiên tai

- Động đất
- Bão, lũ lụt
- Cháy nổ
- Thời tiết

Con người

- Lỗi do nhân viên vận hành
- Quản lý và xử lý mật khẩu không phù hợp
- Bất cẩn trong bảo quản/xử lý thông tin, dữ liệu
- Mất máy tính, thiết bị di động
- Thiếu nhận thức về ATTT

Kỹ thuật

- Mất điện, điện không ổn định
- Lỗi cơ sở dữ liệu
- Mất dữ liệu do thiếu dung lượng lưu trữ
- Gián đoạn dữ liệu
- Ngắt kết nối mạng
- Hỏng hóc phần cứng
- Lỗi phần mềm

Tấn công có chủ đích

- Trộm cắp thiết bị
- Sử dụng hoặc sửa đổi dữ liệu trái phép
- Sử dụng phần mềm độc hại
- Gây rò rỉ thông tin
- Sử dụng dịch vụ trái phép
- Sử dụng phần mềm trái phép /không đúng cách
- Giả mạo danh tính
- Nghe trộm
- Truy cập mạng trái phép

03

Một số hậu quả từ các sự cố ATTT

Hậu quả đối với Công ty

Mất lòng tin và độ uy tín của Công ty

Vướng vào những rắc rối, vụ kiện tụng

Ảnh hưởng đến doanh thu của Công ty

Mất đi cơ hội cạnh tranh và đầu tư

CONFIDENTIAL

Nguy cơ vi phạm pháp luật

Điểm a khoản 5 Điều 63 Nghị định số 98/2020/NĐ-CP ngày 03 tháng 02 năm 2020

Phạt tiền từ 30.000.000 đồng đến 40.000.000 đồng đối với Đánh cắp, tiết lộ, chuyển nhượng, bán các thông tin liên quan đến bí mật kinh doanh của thương nhân, tổ chức khác hoặc thông tin cá nhân của người tiêu dùng trong thương mại điện tử khi chưa được sự đồng ý của các bên liên quan.

Điểm b khoản 1 điều 226 Bộ luật hình sự được sửa đổi, bổ sung năm 2009

Phạt tiền từ 10-100 triệu đồng đối với Hành vi mua bán, trao đổi, tặng cho, sửa chữa, thay đổi hoặc công khai hóa những thông tin riêng hợp pháp của cơ quan, tổ chức, cá nhân khác trên mạng máy tính, mạng viễn thông, mạng Internet mà không được phép của chủ sở hữu thông tin.

CONFIDENTIAL

04

GEM
YOUR TRUSTED PARTNER

Hệ thống quản lý An toàn thông tin (ISMS)

CONFIDENTIAL

Hệ thống quản lý ATTT

Hệ thống quản lý an toàn thông tin (Information Security Management System - ISMS)

Là một hệ thống bảo gồm các hướng dẫn để áp dụng quy trình, kỹ thuật và nguồn lực nhằm giúp tổ chức bảo vệ và quản lý thông tin thông qua quản lý rủi ro.
Hệ thống ISMS tập trung quản lý và bảo vệ 3 tính chất trọng yếu của thông tin: C-I-A

Tiêu chuẩn ISO/IEC 27001:2013

GEM áp dụng tiêu chuẩn để thiết lập, vận hành, triển khai, theo dõi, xem xét, duy trì và quản lý hệ thống ISMS hiệu quả

Chứng chỉ của GEM

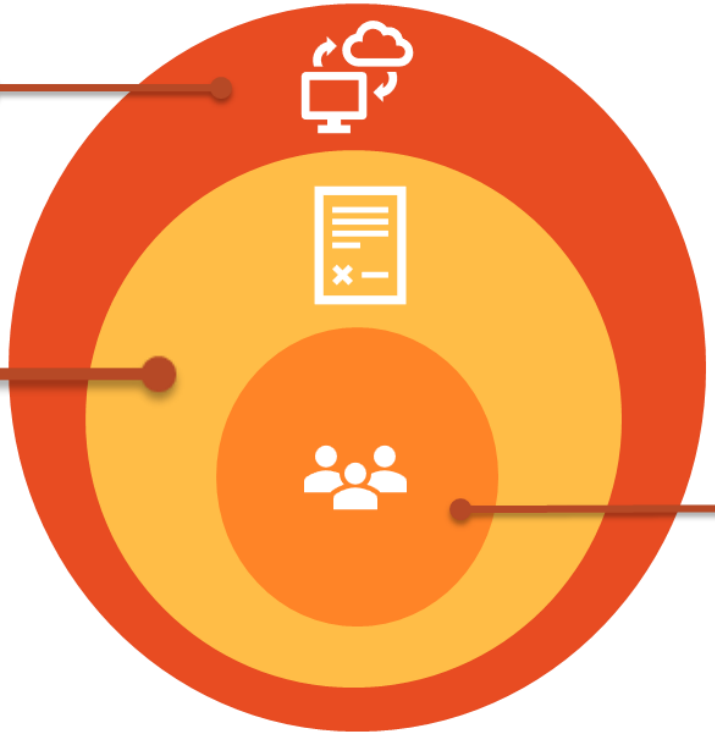
Hằng năm, GEM được đánh giá, cấp và duy trì chứng nhận áp dụng tiêu chuẩn ISO/IEC 27001:2013 bởi tổ chức DAS Việt Nam.
Chứng chỉ ISO/IEC 27001 của GEM có giá trị trong vòng 3 năm.

Hệ thống quản lý ATTT

GEM
YOUR TRUSTED PARTNER

KỸ THUẬT - CÔNG NGHỆ

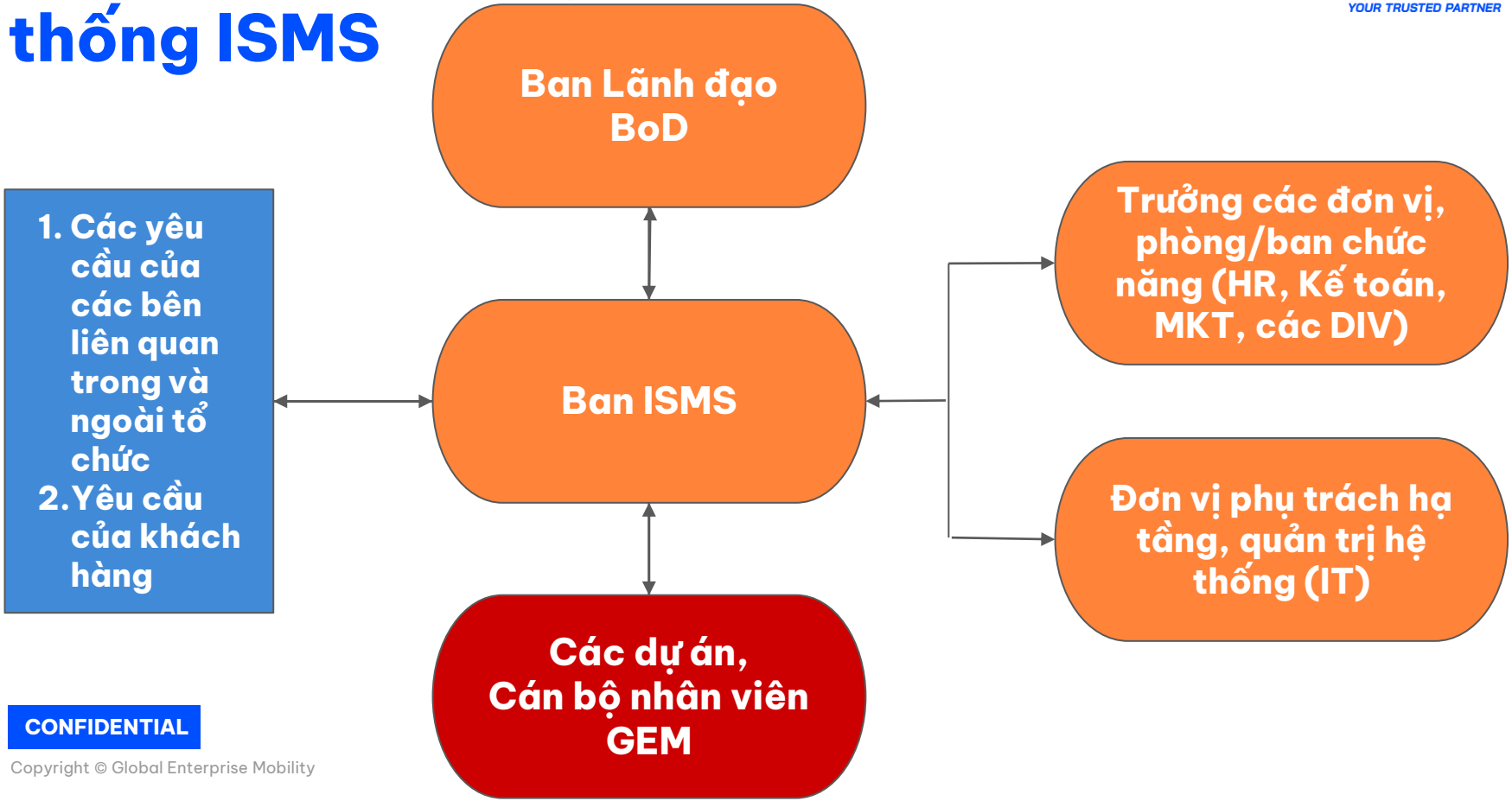
VĂN BẢN - CHÍNH SÁCH



CON NGƯỜI

Mắt xích yếu nhất trong Hệ thống ISMS

Sơ đồ cấu trúc Hệ thống ISMS



CONFIDENTIAL

Báo cáo khi phát hiện sự kiện/ sự cố

- Một số ví dụ về sự cố ATTT:
  - Máy trạm/ máy chủ bị nhiễm virus
  - Phát hiện thay đổi trái phép trên các hệ thống
  - Không truy cập đường Internet hoặc các hệ thống thông tin
  - Phát hiện dữ liệu bị sửa đổi trái phép

- Khi phát hiện hoặc nghi ngờ có sự cố ATTT xảy ra
  -> Thông báo ngay tới một trong số các kênh sau đây:
  1) Hòm thư: isms@gemvietnam.com
  2) Đại diện Ban ISMS: anh Nguyễn Sỹ Huy

Sự kiện/ sự cố ATTT

Sự kiện ATTT: là sự thay đổi có thể quan sát được so với trạng thái ổn định của hệ thống

Sự cố ATTT: một hoặc một chuỗi các **sự kiện ATTT không mong muốn** có khả năng làm **tổn hại đến các tài sản thông tin hoặc hoạt động sản xuất, kinh doanh** của GEM, đe dọa làm ảnh hưởng đến cán bộ nhân viên, khách hàng hoặc đối tác của GEM.

Phân loại sự cố ATTT

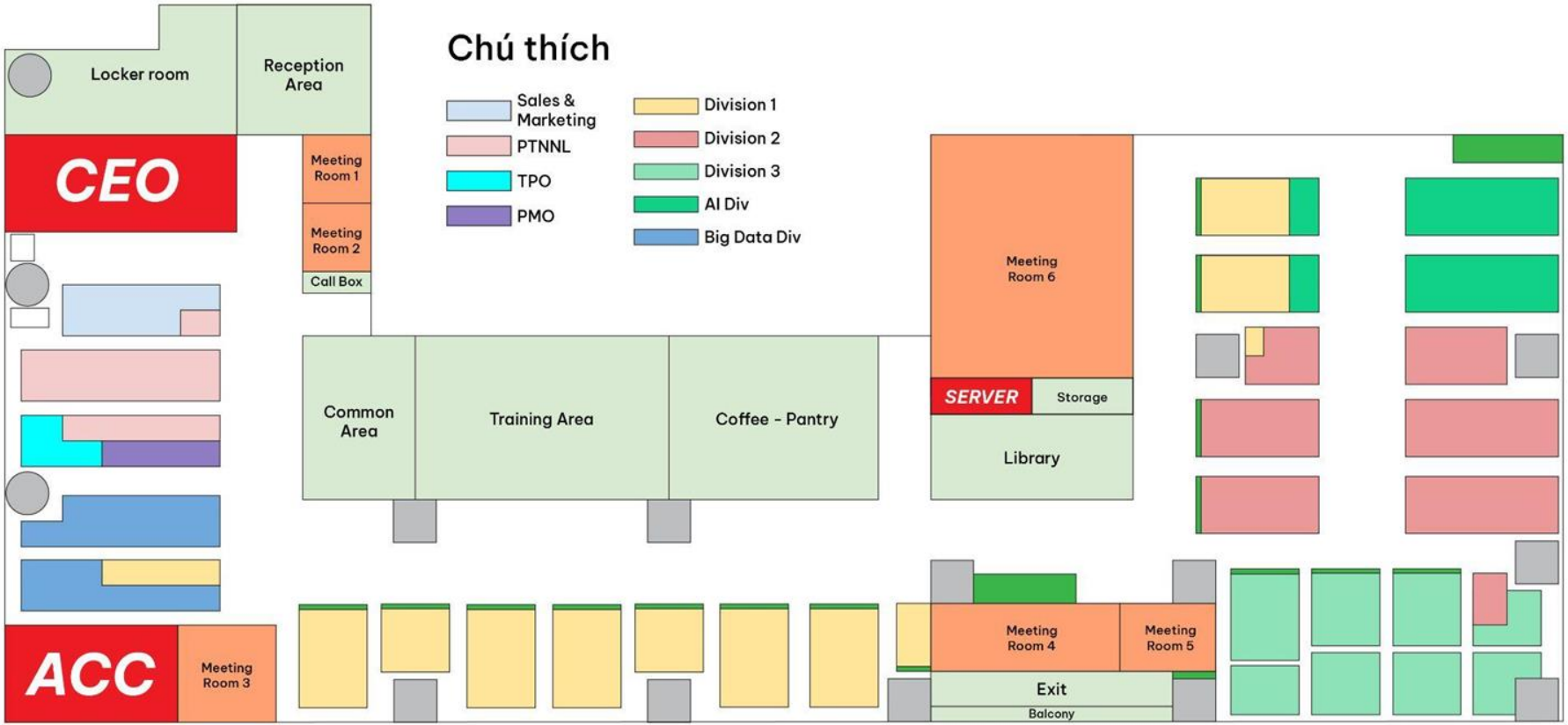
GEM
YOUR TRUSTED PARTNER

(1) Phát hiện virus hoặc bị virus tấn công	(7) Sự cố về mạng
(2) Mất thiết bị lưu trữ thông tin	(8) Sự cố về phần cứng
(3) Phát hiện truy cập trái phép	(9) Sự cố về phần mềm
(4) Vi phạm các luật sở hữu trí tuệ	(10) Tiết lộ trái phép thông tin
(5) Phản hồi của Khách hàng liên quan đến ATTT	(11) Sửa đổi hoặc hủy trái phép thông tin
(6) Lỗ hổng An toàn thông tin	

05

Chính sách, quy định ATTT cần tuân thủ

Quy định ATTT vành đai vật lý



Thẻ nhân viên

- Sử dụng thẻ nhân viên để ra vào Văn phòng GEM, đóng cửa sau khi ra vào
- Đeo thẻ nhân viên trong suốt thời gian làm việc tại Văn phòng GEM
- **KHÔNG MƯỢN** và **CHO MƯỢN** thẻ
- **KHÔNG** mở cửa hộ, chú ý **KHÔNG** để người khác đi theo sau khi mở cửa

Tài khoản truy cập

KHÔNG CHIA SẺ tài khoản truy cập các hệ thống thông tin cho bất kỳ ai (kể cả lãnh đạo, quản lý, cấp trên).

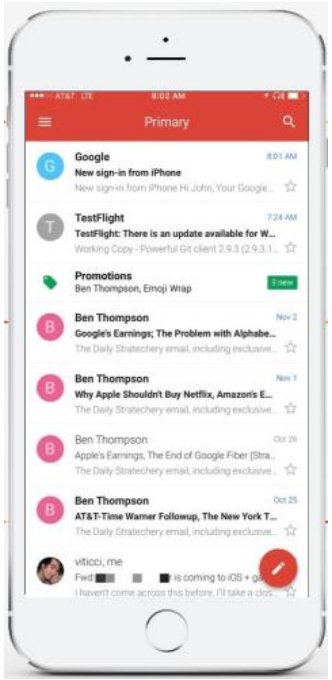
THIẾT LẬP MFA (**M**ulti-**F**actor **A**uthentication) cho tài khoản (nếu có) .

Sử dụng Email

Kiểm tra kỹ các trường To, CC, BCC, tệp đính kèm và nội dung email trước khi gửi

Cảnh giác với các email có dấu hiệu lừa đảo

Đặt mật khẩu cho file đính kèm chứa thông tin mật, gửi mật khẩu file đính kèm bằng phương thức khác



KHÔNG sử dụng email công việc vào mục đích cá nhân

KHÔNG chia sẻ mật khẩu email cho bất kỳ ai dưới bật kỳ hình thức nào

KHÔNG gửi các email spam, email quảng cáo

CONFIDENTIAL

Bảo mật mật khẩu

GEM
YOUR TRUSTED PARTNER

Độ phức tạp

Ít nhất 8 ký tự gồm: chữ hoa, chữ thường, số và ký tự đặc biệt.
KHÔNG chứa tên account của người dùng hoặc 1 phần tên đầy đủ có đội dài hơn 2 ký tự

Lịch sử mật khẩu

Mật khẩu mới không trùng với 2 mật khẩu gần nhất trước đó

Thời hạn mật khẩu

Thay đổi mật khẩu định kỳ mỗi 60 ngày

Khi nghi ngờ bị lộ mật khẩu

Thay đổi mật khẩu ngay lập tức khi nghi ngờ mật khẩu bị lộ hoặc tài khoản bị truy cập không cho phép

Bảo mật mật khẩu

Dùng chung mật khẩu

KHÔNG dùng chung mật khẩu cho nhiều tài khoản (công việc, mạng xã hội, thanh toán...)

Viết mật khẩu ra giấy

KHÔNG ghi chép mật khẩu ra giấy hoặc tệp văn bản

Nhớ mật khẩu

KHÔNG sử dụng tính năng ghi nhớ mật khẩu trên trình duyệt

Chia sẻ mật khẩu

Tuyệt đối KHÔNG chia sẻ mật khẩu cho bất kỳ ai dưới bất kỳ hình thức nào

CONFIDENTIAL

Bảo mật mật khẩu

Một số cách ghi nhớ mật khẩu an toàn

Trong trường hợp có quá nhiều tài khoản/mật khẩu cần ghi nhớ, chúng ta có thể sử dụng một số cách ghi nhớ mật khẩu an toàn sau:

- Liệt kê các tài khoản mật khẩu vào tệp văn bản và đặt mật khẩu cho tệp này
- Sử dụng các phần mềm ghi nhớ mật khẩu đánh tin cậy

Lưu ý khi sử dụng Internet

GEM
YOUR TRUSTED PARTNER

Chặn quảng cáo
Cài đặt tính năng chặn quảng cáo (Adblock) trên trình duyệt

Lừa đảo trên internet


KHÔNG ấn vào các đường link lạ, truy cập vào các trang web không rõ nguồn gốc hoặc làm theo các email có dấu hiệu lừa đảo

Sử dụng trình duyệt an toàn
Sử dụng các trình duyệt web an toàn như Google Chrome, Firefox, Safari

Chia sẻ thông tin bảo mật


HẠN CHẾ chia sẻ thông tin cá nhân trên Internet, KHÔNG sao chép, gửi các thông tin, dữ liệu bảo mật của Công ty ra ngoài

CONFIDENTIAL

Cài đặt và sử dụng phần mềm

GEM
YOUR TRUSTED PARTNER

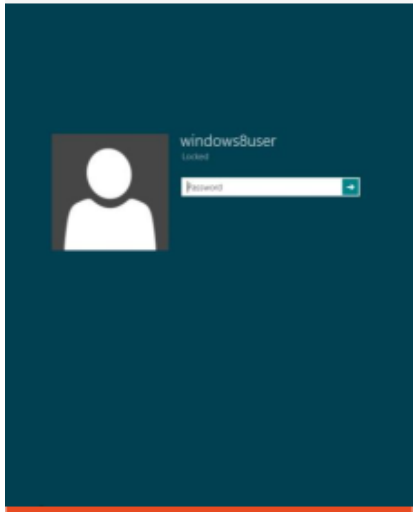
Diệt virus
Cài đặt, cập nhật phần mềm virus và bật chế độ Real time Protection trên máy tính công việc

Hệ điều hành
Đặt chế độ tự động cập nhật Hệ điều hành

Phần mềm ngoài danh mục
KHÔNG cài đặt các phần mềm ngoài danh mục mà chưa có sự cho phép của quản trị hạ tầng

Dùng phần mềm crack
KHÔNG tải, cài đặt và sử dụng các phần mềm vi phạm bản quyền, phần mềm không rõ nguồn gốc

Chính sách “Bàn sạch – Màn sạch”



Khóa/tắt máy tính khi rời khỏi chỗ ngồi

Dọn sạch bàn làm việc, cất tài liệu vào tủ có khóa khi rời khỏi chỗ ngồi

Hủy tài liệu bảo mật trước khi vứt bỏ

ATTT tại các khu vực chung

Tránh để quên tài liệu, tài sản tại các khu vực chung: phòng họp, khu vực ăn, khu vực máy in/photocopy, khu vệ sinh ...

CONFIDENTIAL

Lưu trữ dữ liệu

Dữ liệu bản cứng

- Được lưu trong tủ có khóa
- Được quản lý bởi cán bộ quản lý hồ sơ của bộ phận/dự án

Dữ liệu bản mềm

- Tài liệu sau khi phê duyệt/bàn giao phải được lưu trữ trên các hệ thống thông tin chung của GEM (Google Drive, Confluence)
- Source code phải được lưu trên BitBucket

An toàn mạng

CẤM TUYỆT ĐỐI việc cắm các thiết bị thu phát sóng vào mạng nội bộ của GEM.

Đăng ký sử dụng máy tính cá nhân

Đăng ký và thời hạn

Cán bộ có nhu cầu phải đăng ký sử dụng máy tính cá nhân với IT GEM. Thời hạn sử dụng máy tính cá nhân: 1 năm

Dán nhãn tài sản cá nhân

Máy tính cá nhân phải được dán nhãn tài sản cá nhân trước khi sử dụng tại GEM

Cài đặt phần mềm

Cài đặt phần mềm diệt virus theo quy định của GEM

Chỉ cài đặt các phần có bản quyền, đáng tin cậy

Máy đã cài lại HĐH

Nếu cài lại HĐH máy phải qua IT kiểm tra, phê duyệt trước khi sử dụng tại GEM

Bảo lãnh khách

- Đăng ký thông tin khách hàng, đối tác với Bộ phận Hành chính để làm việc tại GEM
- Chỉ tiếp đón khách tại Khu vực sảnh hoặc phòng họp
- Không dẫn khách vào khu vực làm việc khi chưa đăng ký với Bộ phận Hành chính

An toàn thông tin đối với dự án

- **KHÔNG** chia sẻ, upload mã nguồn (source code) và các tài liệu dự án khác lên Github, Drive và các kênh chia sẻ dữ liệu khác
- **KHÔNG** lưu dữ liệu dự án, source code trên máy tính cá nhân
- **KHÔNG** sử dụng mã nguồn mở, không rõ nguồn gốc trừ trường hợp được cho phép
- **KHÔNG** xâm phạm thông tin cá nhân của Khách hàng hoặc người sử dụng sản phẩm, sử dụng thông tin Khách hàng làm dữ liệu test
- **KHÔNG** chia sẻ bất kỳ thông tin nào về dự án, khách hàng trên các trang mạng xã hội, CV xin việc hoặc Linkedin
- **KHÔNG** lưu username, password thông tin đăng nhập, token vào source code (fixed code)
- **KHÔNG** sử dụng Database có dữ liệu khách hàng import vào hệ thống test/staging

THANK YOU!

GEM Corporation: 3rd floor, The Nine Building, no.9 Pham Van Dong Street, Cau Giay District, Ha Noi, Viet Nam

(84) 24 6 664 0520

gemvietnam.com