

CÔNG TY TNHH ICETEA SOFTWARE



Icetea **Software**

**TÀI LIỆU ĐÀO TẠO NHẬN THỨC
AN TOÀN THÔNG TIN TẠI ITS
(theo Tiêu chuẩn ISO/IEC 27001:2022)**

[Đối tượng tham gia: Cán bộ nhân viên và cấp quản lý]

30.07.2025

Ban ISO

Internal use



Đối tượng bắt buộc tham gia:

- Toàn thể Cán bộ Nhân viên của Icetea Software trên tất cả các phòng ban, cấp bậc.
- Đây là chương trình đào tạo bắt buộc.



Đơn vị tổ chức: Ban ISO



Thời gian triển khai: 04/08/2025 đến 05/09/2025.



Cách thức thực hiện:

- **Tổ chức đào tạo:** Học lý thuyết (Nghe video hoặc đọc tài liệu tham khảo file PDF) + làm bài test.
- **Chương trình đào tạo:** Tổ chức theo tuần, triển khai liên tục trong 5 tuần. Mỗi tuần, học viên sẽ được cung cấp: Video bài học + Tài liệu PDF tham khảo + Bài test.
- **Thời gian tham gia:** Thành viên chủ động thu xếp thời gian tham gia học lý thuyết và làm bài test.



Tiêu chí hoàn thành: Hoàn thành bài test ĐÚNG thời hạn và ĐẠT tối thiểu.

- **Đúng thời hạn:** Hoàn thành và gửi lại bài test muộn nhất trước 24h chủ nhật hàng tuần.
- **Đạt tối thiểu:** Bài test mỗi tuần gồm 5 câu hỏi. **Làm đúng 4/5 câu là ĐẠT bài test.** Thành viên có tối đa 3 lần làm bài test.
- **Lưu ý:** Đối với các trường hợp không hoàn thành sau 03 lần, Ban ISO sẽ tổng hợp và gửi thông tin đến Quản lý trực tiếp để nhận được sự hỗ trợ, đôn đốc kịp thời.



1. Giới thiệu Chứng nhận về ATTT tại ITS
2. Mục tiêu và lợi ích tuân thủ ATTT
3. Giới thiệu chung về Thông tin và ATTT
4. Quy định về ATTT ở ITS
5. Trách nhiệm tuân thủ ATTT của quản lý và nhân viên ITS



1. GIỚI THIỆU CHỨNG NHẬN VỀ ATTT TẠI ITS



ITS đánh giá ISO 27001 lần đầu ngày 05.06.2025 và đạt điều kiện lấy chứng nhận ISO/IEC 27001:2022 về Bảo mật An toàn thông tin



Lĩnh vực chứng nhận: Sản xuất và Gia công phần mềm cho thị trường trong nước và quốc tế



Chứng nhận được cấp bởi: Tổ chức chứng nhận quốc tế SMG





ISO 27001:2022 là tiêu chuẩn quốc tế về hệ thống quản lý an toàn thông tin (ISMS - Information Security Management System) theo phiên bản mới nhất (phiên bản 2022) của tiêu chuẩn do Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) và Ủy ban Kỹ thuật Điện Quốc tế (IEC) ban hành.



2. MỤC TIÊU VÀ LỢI ÍCH CỦA ATTT



**TẠI SAO CẦN TUÂN
THỦ TIÊU CHUẨN VỀ BẢO
MẬT ATTT TẠI ITS ???**



**CÁC CASE
STUDIES**

Ransomware là một loại phần mềm độc hại (malware) mà kẻ tấn công sử dụng để mã hóa dữ liệu của bạn, hoặc khóa máy tính của bạn, và yêu cầu bạn trả tiền chuộc (ransom) để có thể truy cập lại được dữ liệu hoặc hệ thống của mình. Nói cách khác, ransomware là một hình thức tống tiền trên không gian mạng, trong đó tội phạm mạng sử dụng công nghệ để tống tiền nạn nhân.



Dương Thanh Hải

12 Tháng 3, 2020 · 



"It's not safe to stay home!"

Một dòng cảnh báo của một loại mã độc tống tiền (Ransomware) trong thời dịch Corona.

Trong thời đại công nghệ phát triển như hiện tại thì ở nhà cũng dễ dàng bị lừa đảo trực tuyến hoặc nhiễm các loại Virus máy tính.

Cùng cập nhật vài cách lừa đảo trực tuyến đơn giản nhưng ... không thiếu trường hợp người dùng bị lừa.

Công ty 158 tuổi sụp đổ do nhân viên đặt mật khẩu yếu

ANH- Knights of Old (KNP), công ty vận tải với lịch sử hoạt động lâu dài, phải đóng cửa sau cuộc tấn công mã độc tống tiền (ransomware) vào năm 2023.

Chương trình *Panorama* của BBC phát sóng tuần này kể lại sự cố diễn ra giữa năm 2023 của KNP để cảnh báo về mối nguy hiểm của mã độc tống tiền.

Nhóm tội phạm mạng Akira được cho là đã truy cập hệ thống của KNP thông qua mật khẩu dễ đoán do một nhân viên sử dụng. Sau đó, tin tặc mã hóa và khóa dữ liệu hoạt động của KNP, thông báo cách duy nhất để mở khóa dữ liệu là trả tiền. Thông điệp đòi tiền chuộc có nội dung: "Nếu đang đọc những dòng này, cơ sở hạ tầng nội bộ của công ty bạn đã bị phá hủy một phần hoặc hoàn toàn... Hãy giữ nước mắt, sự oán giận và cố gắng tạo một cuộc đối thoại mang tính xây dựng".

Case studies 3 - Phishing - unicode domain



Icetea Software

Phishing sử dụng tên miền Unicode, còn gọi là tấn công homoglyph IDN, là một hình thức lừa đảo trực tuyến trong đó kẻ tấn công tạo ra các tên miền trông giống hệt tên miền hợp pháp nhưng sử dụng các ký tự Unicode từ các bảng chữ cái khác nhau. Mục tiêu là lừa người dùng truy cập vào các trang web giả mạo, từ đó đánh cắp thông tin nhạy cảm.


The screenshot shows a web browser window with the address bar displaying `https://myetherwalleT.com/#contracts`. The page content includes a transaction ID `0xd0a6E6C54DbC68Db5db3A091B171A77407Ff7ccf` and a section titled "1. Claim block.one EOS Tokens" with instructions to select `claimAll`, unlock the wallet, and send a transaction with a gas limit of at least 90000. Below this is a "claimAll" button. At the bottom, there is a section "How would you like to access your wallet?" with radio button options: MetaMask / Mist, Ledger Wallet, TREZOR, Digital Bitbox, Keystore / JSON File, Mnemonic Phrase, Private Key (selected), and Parity Phrase. To the right of this is a section titled "Paste Your Private Key" with a warning that this is not a recommended way to access the wallet and a list of recommended methods: MetaMask or A Hardware Wallet or Running MEW Offline & Locally, and Learning How to Protect Yourself and Your Funds. It also includes a warning to double-check the URL & SSL cert, stating it should say `https://www.myetherwallet.com` & `MYETHERWALLET LLC [US]` in the URL bar. A large empty text box is provided for pasting the private key.

Case studies 4 - Malware - Extension



Icetea Software

Malware là viết tắt của “malicious software” (phần mềm độc hại): Đây là một thuật ngữ bao trùm, chỉ bất kỳ chương trình hay đoạn mã nào được tạo ra với mục đích gây hại cho hệ thống máy tính, máy chủ, hoặc mạng máy tính. Mục tiêu của chúng rất đa dạng, từ đánh cắp dữ liệu, phá hoại hệ thống cho đến theo dõi người dùng.

Name	Date modified	Type	Size
 Video.3625943.mp4.exe	12/18/2017 10:29 ...	Application	952 KB

```
Func akvzohddz()  
    While 1  
        If FileExists($zpcxxoddutz & "\" & "worker.exe" AND FileExists($zpcxxoddutz & "\" & "config.json") Then  
            If NOT ProcessExists("worker.exe") Then  
                Run($zpcxxoddutz & "\" & "worker.exe", NULL , @SW_HIDE)  
            EndIf  
        EndIf  
        Sleep(5000)  
    WEnd  
EndFunc
```

Chạy chương trình “đào” tiền ảo Monero trên máy bị nhiễm

Malware - Open file có nghĩa là một tệp tin (file) chứa mã độc (malware) được thiết kế để lây nhiễm và gây hại cho máy tính khi người dùng mở tệp đó.

Chia sẻ trên buổi livestream, Độ Mixi cho biết tin tặc đã gửi đến hộp thư của anh một email giả mạo nhà phát hành game, bên trong đính kèm file có chứa mã độc keylogger (phần mềm gián điệp đọc nội dung gõ từ bàn phím). Dựa vào mã độc này, hacker đã lấy được thông tin đăng nhập các tài khoản trực tuyến của Độ Mixi và chiếm quyền điều khiển.



Email giả mạo nhà phát hành game với nội dung đề nghị hợp tác, có kèm theo file chứa mã độc (Ảnh: Độ Mixi).

Case studies 6- Airdrop fake tokens



Icetea Software

Airdrop token giả (fake tokens airdrop) là các chương trình phân phối token tiền điện tử miễn phí được tạo ra bởi những kẻ lừa đảo nhằm mục đích đánh cắp thông tin cá nhân, khóa riêng tư hoặc tiền của người dùng. Chúng thường sử dụng các chiêu trò tinh vi để mạo danh các dự án tiền điện tử uy tín, hoặc dụ dỗ người dùng kết nối ví của họ với các trang web độc hại để đánh cắp dữ liệu.

Case studies - Airdrop fake tokens

Overview

Logs (200)

State

Comments

Transaction Hash:

0x8381106316a36b8552ef36fe72576b50396de4d15f1ce0376cb9949b1739ef48

Status:

Success

Block:

15121945

419 Block Confirmations

Timestamp:

1 hr 29 mins ago (Jul-11-2022 02:50:15 PM +UTC)

Confirmed within 30 secs

From:

0x24a4b33bfa8e32b3456f95381de429c11c2c6fd6

Interacted With (To):

Contract 0xcf39b7793512f03f2893c16459fd72e65d2ed00c

Tokens Transferred: 200

From Uniswap V3: Positi... To 0x11b1785d9ac81... For 400 \$ UniswapLP... (Uniswa...)

From Uniswap V3: Positi... To 0x11b24ba0f63e6... For 400 \$ UniswapLP... (Uniswa...)

From Uniswap V3: Positi... To 0x11b2ac1d729cd... For 400 \$ UniswapLP... (Uniswa...)

From Uniswap V3: Positi... To 0x11b31ad943481... For 400 \$ UniswapLP... (Uniswa...)

From Uniswap V3: Positi... To 0x11b38e8b2502d... For 400 \$ UniswapLP... (Uniswa...)

From Uniswap V3: Positi... To 0x11b50686d3983... For 400 \$ UniswapLP... (Uniswa...)

From Uniswap V3: Positi... To 0x11b67a503b3b7... For 400 \$ UniswapLP... (Uniswa...)

From Uniswap V3: Positi... To 0x11b6a5fe2906f3... For 400 \$ UniswapLP... (Uniswa...)

From Uniswap V3: Positi... To 0x11b6b67de481a... For 400 \$ UniswapLP... (Uniswa...)

From Uniswap V3: Positi... To 0x11b7e01c575e0... For 400 \$ UniswapLP... (Uniswa...)

Value:

0 Ether (\$0.00)

Transaction Fee:

0.016438072407915059 Ether (\$18.80)

Gas Price:

0.00000002777947077 Ether (27.777947077 Gwei)

KẾT LUẬN:

Từ các Case studies về sự cố an toàn thông tin trong thực tế cho thấy:

** Thông tin có thể bị đánh cắp, mất mát hoặc rò rỉ bất cứ lúc nào nếu không có biện pháp bảo vệ phù hợp.*


** Mất hợp đồng, mất khách hàng, thiệt hại nghiêm trọng (phải đền bù thiệt hại cho khách hàng)...*

👉 Vì vậy, công ty cần thiết lập, áp dụng và tuân thủ hệ thống đảm bảo An Toàn Thông Tin

👉 Sau đây là Mục tiêu và lợi ích tuân thủ ATTT

- 1. Nâng cao nhận thức về an toàn thông tin*
- 2. Giảm thiểu rủi ro do lỗi con người*
- 3. Trang bị kỹ năng thực hành bảo mật*
- 4. Góp phần xây dựng văn hóa bảo mật trong ITS*
- 5. Tăng khả năng phản ứng khi có sự cố*
- 6. Tuân thủ các quy định pháp luật và tiêu chuẩn*



 **1. Bảo vệ tài sản và giảm rủi ro:** Ngăn chặn rò rỉ dữ liệu, bảo vệ tài sản và phần mềm khỏi truy cập trái phép, phá hoại

- Dữ liệu khách hàng, hợp đồng, mã nguồn, tài liệu tài chính là những tài sản cực kỳ giá trị.
- Nếu bị rò rỉ hoặc mất mát có thể gây tổn thất nghiêm trọng về tài chính và pháp lý.

 **2. Tạo niềm tin với khách hàng và đối tác nâng cao nhận thức nội bộ**

- Doanh nghiệp có hệ thống bảo mật tốt thường được đánh giá cao về độ uy tín và mức độ an toàn.
- Có lợi thế hơn khi đàm phán hợp đồng, nhất là trong dự án phần mềm, tài chính, chăm sóc sức khỏe, ngân hàng...

 **3. Hỗ trợ chuyển đổi số và phát triển bền vững:** Giúp Công ty phát triển bền vững trong môi trường số nhiều rủi ro.

Chuyển đổi số làm tăng mức độ phụ thuộc vào công nghệ (Cloud, IoT, AI, SaaS...). Nếu không có ATTT, hệ thống dễ bị tấn công mạng, mất dữ liệu, rò rỉ thông tin.

 **4. Tuân thủ pháp luật và các tiêu chuẩn:** Tránh các rủi ro pháp lý.

Tuân thủ hợp đồng với khách hàng có yêu cầu bảo mật.

- Nhiều Khách hàng yêu cầu Nhà cung cấp sản phẩm/ dịch vụ bắt buộc tuân thủ các quy định ATTT như:
 - ✓ Luật An ninh mạng, Luật bảo vệ dữ liệu cá nhân (PDPA), Nghị định 13/2023/NĐ-CP...
 - ✓ Các chuẩn quốc tế: ISO/IEC 27001,...



Thông tin là gì?
ATTT là gì?

3. GIỚI THIỆU CHUNG VỀ THÔNG TIN VÀ ATTT

- **Định nghĩa thông tin:**

Thông tin là sự hiểu biết của con người về một sự kiện, một hiện tượng nào đó thu nhận được từ nhiều cách khác nhau qua nghiên cứu, trao đổi, nhận xét, học tập, truyền thụ, cảm nhận...

Một số ví dụ về Thông tin:

- ✓ Thông tin dự án: Hồ sơ khách hàng, hồ sơ dự án, danh sách thành viên dự án, hồ sơ năng lực triển khai dự án, đo lường độ hài lòng của khách hàng, Tiến độ dự án...
- ✓ Ghi chú nội dung góp ý; Biên bản họp
- ✓ Kiến thức sau đào tạo, kinh nghiệm làm việc.



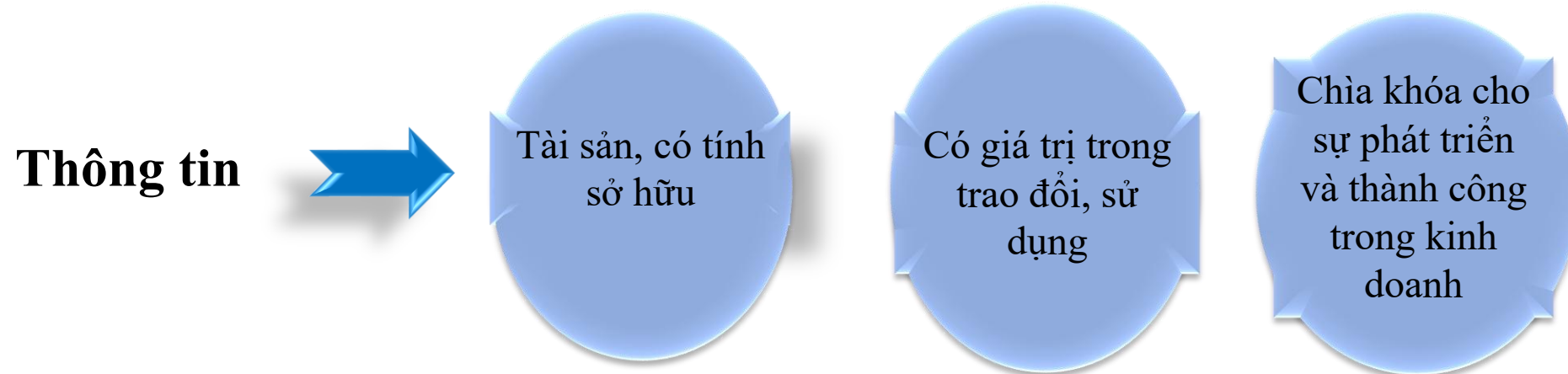
- **Cách thông tin thường được ghi/lưu trữ:**

- a) Được lưu trữ trong não bộ của con người: Được ghi nhớ thông qua học tập, quan sát...
- b) Được in hoặc viết ra giấy: tài liệu, hóa đơn, hợp đồng, ghi chú...
- c) Được lưu trữ bằng máy tính: Lưu trong ổ cứng, máy chủ, các thiết bị số khác.
- d) Được lưu trên không gian mạng: Cloud, Email, website, hệ thống lưu trữ trực tuyến, mạng xã hội...



- **Cách Thông tin thường được truyền/phát ra ngoài:**

- a) Được trao đổi qua lời nói, cử chỉ hành động: Nói chuyện, họp nhóm, thảo luận, ngôn ngữ cơ thể (gật đầu, lắc đầu...),...
- b) Được trao đổi qua mạng Internet: Mail, Zalo, Teams, Messenger, Telegram, Zoom chat...
- c) Được trao đổi qua các phương tiện viễn thông: Gọi điện thoại, hội nghị truyền hình, truyền hình trực tiếp...
- d) Được trình chiếu khi thuyết trình: Trình bày PowerPoint trong cuộc họp, hội thảo, lớp học...



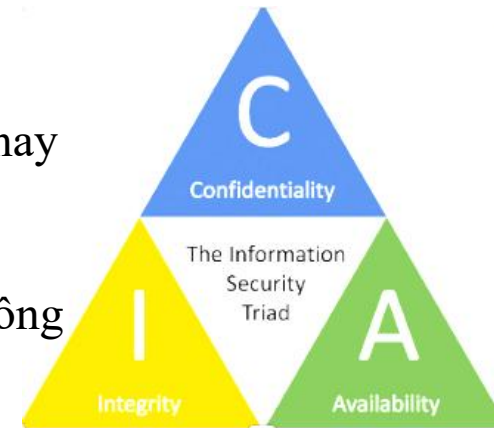
1. Thông tin là **tài sản** của Công ty.
2. Thông tin là đầu vào để giúp lãnh đạo điều hành, quản lý Công ty nên sẽ quyết định sự thành công hay thất bại của Công ty.
3. Thông tin giúp cho việc hoạch định kế hoạch kinh doanh và thực hiện kế hoạch đó hiệu quả.

❖ **KHÁI NIỆM**: ATTT được hiểu là một hành động **phòng ngừa, ngăn chặn hoặc ngăn cản** sự truy cập, sử dụng, chia sẻ, phát tán hoặc phá hủy những Thông Tin khi chưa được sự cho phép của chủ sở hữu. Hay một cách then chốt ATTT chính là chìa khóa của tiêu chuẩn **ISO/IEC 27001:2022**



❖ **AN TOÀN THÔNG TIN** là duy trì tính **bảo mật**, tính **trọn vẹn** và tính **sẵn sàng** của thông tin:

- Tính **Bảo mật (Confidentiality)** là đảm bảo thông tin chỉ được tiếp cận bởi những người được cấp quyền tương ứng.
- Tính **Trọn vẹn (Integrity)** là bảo vệ sự chính xác, hoàn chỉnh của thông tin và thông tin chỉ được thay đổi bởi những người được cấp quyền.
- Tính **Sẵn sàng (Availability)** của thông tin là những người được quyền sử dụng có thể truy xuất thông tin khi họ cần.



An toàn thông tin sẽ giúp kiểm soát và bảo vệ thông tin tránh khỏi việc **vô tình hoặc cố ý thay đổi, xóa cũng như tiết lộ** thông tin không được phép.

QUY ĐỊNH VỀ TÀI SẢN THÔNG TIN

❖ Tài sản được phân thành 5 loại như sau:



1. Tài sản thông tin:

- *Hợp đồng, thỏa thuận pháp lý.*
- *Hồ sơ giấy tờ* của công ty, các *biên bản họp quan trọng*.
- *Các bản in* của thiết kế, kế hoạch.
- *Thông tin khách hàng:* Dữ liệu cá nhân, lịch sử giao dịch, thông tin liên lạc.
- *Thông tin tài chính:* Báo cáo tài chính, dữ liệu kế toán, thông tin giao dịch ngân hàng.
- *Sở hữu trí tuệ:* Bí mật kinh doanh, công thức, bản quyền, bằng sáng chế, thiết kế sản phẩm, mã nguồn phần mềm.
- *Thông tin nhân sự:* Hồ sơ nhân viên, thông tin lương thưởng, đánh giá hiệu suất.
- *Dữ liệu hoạt động:* Kế hoạch kinh doanh, chiến lược marketing, quy trình vận hành, dữ liệu nghiên cứu và phát triển (R&D).



2. Tài sản phần mềm:

- **Phần mềm:** Hệ điều hành, phần mềm ứng dụng (CRM, ERP), hệ quản trị cơ sở dữ liệu, các ứng dụng tự phát triển



3. Tài sản vật lý :

- Các thiết bị kỹ thuật, thiết bị CNTT, tủ đựng tài liệu.
- **Phần cứng:** Máy chủ (servers), máy tính cá nhân (PCs), thiết bị mạng (routers, switches), thiết bị lưu trữ (ổ cứng, USB).



4. Tài sản dịch vụ - công nghệ: Các dịch vụ cung cấp ứng dụng, tài khoản, cloud, cung cấp thiết bị CNTT, dịch vụ tòa nhà, đường truyền internet.



5. Tài sản con người (nhân sự công ty): Nhân viên ký hợp đồng với Công ty.

STT	Dấu hiệu	Định nghĩa	Ví dụ
1	Tuyệt mật (Secret)	<p>Là thông tin quan trọng mà nếu thông tin bị rò rỉ sẽ làm giảm uy tín và sức cạnh tranh của công ty.</p> <p>- Không được tiết lộ cho bất kỳ ai khác ngoài những người có liên quan được chỉ định, người thiết lập ra thông tin chịu trách nhiệm chỉ định người có liên quan được tiếp cận thông tin.</p>	<p>Chiến lược kinh doanh của Công ty</p> <p>Các kế hoạch kinh doanh của Công ty</p> <p>Lương, thưởng và Dữ liệu cá nhân</p> <p>Dữ liệu tài chính của Công ty và khách hàng</p>
2	Mật (Confidential)	<p>Thông tin nhạy cảm, mức độ cao mật cao, bảo mật với những thành viên không liên quan</p>	<p>Các hợp đồng mật với khách hàng</p> <p>Thỏa thuận ATTT với khách hàng và các NCC</p> <p>Thông tin cá nhân của Khách hàng và các tài liệu tương tự khác</p> <p>Thông tin dự án</p> <p>Hồ sơ sản xuất và gia công phần mềm</p>
3	Nội bộ (Internal use)	<p>Thông tin được sử dụng trong nội bộ, không tiết lộ cho bên ngoài</p>	<p>Tất cả hoặc 1 nhóm nhân viên có thể truy cập thông tin này trên 1Office hoặc phần mềm, ứng dụng công ty sử dụng</p>
4	Công khai (Public)	<p>Loại thông tin này cho phép công bố công khai trên các phương tiện thông tin đại chúng</p>	<p>Tài liệu quảng cáo bán hàng, chương trình tiếp thị và các thông cáo báo chí, bản tin của công ty, thông tin được công bố trên website của công ty.</p>



4. QUY ĐỊNH AN TOÀN THÔNG TIN TẠI ITS

QUY ĐỊNH ATTT TẠI ITS

- ① • QUY ĐỊNH SỬ DỤNG THÔNG TIN MẬT
- ② • QUY ĐỊNH QUẢN LÝ VÀ SỬ DỤNG TÀI KHOẢN, MẬT KHẨU
- ③ • QUY ĐỊNH VỀ SỬ DỤNG THIẾT BỊ CNTT
- ④ • QUY ĐỊNH VỀ SỬ DỤNG VÀ TRUY CẬP MẠNG NỘI BỘ
- ⑤ • QUY ĐỊNH VỀ SỬ DỤNG EMAIL CÔNG TY
- ⑥ • PHÒNG CHỐNG VIRUS – VẬN CHUYỂN THÔNG TIN - XỬ LÝ SỰ CỐ ATTT
- ⑦ • QUY ĐỊNH VỀ SỬ DỤNG MÁY IN, MÁY HỦY GIẤY, TÀI LIỆU BẢN CỨNG – QUY ĐỊNH RA VÀO CÔNG TY

MỤC ĐÍCH SỬ DỤNG THÔNG TIN

- **Công việc:** Chỉ sử dụng thông tin mật cho công việc liên quan
- **Bảo mật:** Giữ bí mật, không tiết lộ thông tin nội bộ công ty.

TRÁNH SỬ DỤNG SAI MỤC ĐÍCH

- **Mục đích cá nhân:** Không sử dụng thông tin mật cho mục đích cá nhân.
- **Sao chép:** Tuyệt đối không sao chép và lưu trữ công cộng hoặc cá nhân

LƯU TRỮ THÔNG TIN AN TOÀN

- **Thông tin quan trọng lưu trữ trên Cloud hoặc Server của Công ty:** 1Office; Drive; hồ sơ dự án lưu trữ trên Git, Confluence, Jira;...không lưu trữ trên ổ cứng cá nhân hoặc thiết bị di động

BẢO MẬT DỰ ÁN

- **Bảo mật tuyệt đối:** Bảo mật thông tin ở mức cao nhất

TRAO ĐỔI - GIAO TIẾP

- **Không** trao đổi, giao tiếp các nội dung công việc, dự án ngoài khu vực Công ty.
- **Không trao đổi mức lương, bảng lương** cho bất kỳ ai với bất cứ mục đích nào.

2. QUY ĐỊNH QUẢN LÝ VÀ SỬ DỤNG TÀI KHOẢN, MẬT KHẨU



Icetea Software

Thay đổi mật khẩu

- CBNV ngay lần đầu đăng nhập
- Bảo vệ tài khoản đảm bảo bảo mật ATTT

Quản lý tài khoản, mật khẩu

- Hạn chế sử dụng cùng 1 mật khẩu cho nhiều tài khoản
- Tuyệt đối không chia sẻ, cho mượn tài khoản, mật khẩu được cấp bởi Công ty

Bàn giao tài khoản Admin khi nghỉ việc

- HR, IT xác minh toàn bộ danh sách tài khoản quản trị mà cá nhân này đang nắm giữ: thu hồi, đổi mật khẩu, chuyển giao quyền sở hữu, thay đổi số điện thoại (nếu có)
- Nhân sự nghỉ việc bàn giao đầy đủ thông tin truy cập



Quy tắc chung về sử dụng thiết bị

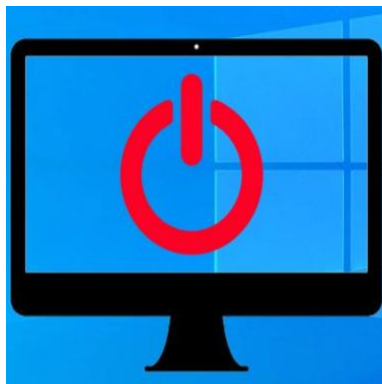
Không tự ý tháo lắp, sửa chữa

Liên hệ IT để được hỗ trợ cài đặt hoặc sửa chữa thiết bị CNTT.



Tắt máy khi ra về

Tắt máy và thiết bị trước khi rời khỏi nơi làm việc. Báo cáo nếu cần bật máy qua đêm.



Khóa máy khi rời vị trí làm việc

Khi rời vị trí làm việc cần khóa máy tính, tránh kẻ gian lợi dụng truy cập trái phép



Không chia sẻ thông tin

Không chia sẻ thông tin từ máy tính cá nhân chưa đăng ký.



Không sử dụng chung máy tính cá nhân.

Để đảm bảo ATTT, mỗi nhân viên phải sử dụng máy tính cá nhân riêng biệt và không chia sẻ thiết bị với người khác



Quản lý phần mềm

Chỉ sử dụng và cài đặt phần mềm có trong danh mục được phép của công ty.

Tuyệt đối không sử dụng hoặc thử nghiệm phần mềm thăm dò, theo dõi, tấn công.

Nghiêm cấm sử dụng các loại phần mềm sử dụng mạng ngang hàng peer-to-peer như Winny, Share, phần mềm xây dựng VPN ảo như SoftEther và phần mềm điều khiển từ xa như VNC trên các thiết bị thông tin như máy tính chứa thông tin mật.

Winny, Share

Phần mềm chia sẻ file P2P

SoftEther

Phần mềm VPN ảo

VNC

Phần mềm điều khiển từ xa

Hạn chế đối với thiết bị cá nhân

CBNV không tự ý mang các thiết bị CNTT (laptop, Ipad, USB...) ra/vào công ty

Đăng ký sử dụng với IT, xin phê duyệt của ban ISO và ký cam kết bảo mật thông tin

Không hoặc hạn chế sử dụng

Thiết bị có khả năng kết nối trực tiếp vào mạng (wire/wireless) hoặc gián tiếp qua máy trạm (wifi router, network card external/usb,...)

Thiết bị có khả năng là vật lưu trữ, trung chuyển dữ liệu (USB,...)

Thiết bị là cầu nối giữa các thiết bị khác (switch, router, các loại converter...)

An toàn thông tin khi làm việc từ xa và Các nguyên tắc cần tuân thủ

Thiết bị làm việc

- Sử dụng **thiết bị được cấp bởi công ty** hoặc đã đăng ký với IT, ban ISO và ký cam kết bảo mật.
- **Khóa màn hình máy tính** khi rời khỏi chỗ.

Kết nối mạng

- **Không sử dụng Wi-Fi công cộng**.
- Ưu tiên dùng Wi-Fi cá nhân có **mật khẩu mạnh** và bảo mật WPA2/WPA3.
- Kết nối qua **VPN công ty** để truy cập hệ thống nội bộ.

Dữ liệu và phần mềm

- **Không lưu trữ dữ liệu nhạy cảm** lên thiết bị cá nhân hoặc cloud cá nhân (Google Drive, Dropbox...).
- **Không cài phần mềm lạ**, chỉ dùng phần mềm được phê duyệt.
- Gửi tài liệu nội bộ qua kênh đã được mã hóa, hạn chế gửi qua email cá nhân.

Quy định làm việc

- Làm việc ở nơi **riêng tư, không bị người khác nhìn vào màn hình**.
- Không chia sẻ thông tin công việc với người không liên quan (kể cả gia đình).
- Tuân thủ chính sách ATTT của công ty như khi làm tại văn phòng.

3. QUY ĐỊNH VỀ SỬ DỤNG THIẾT BỊ CNTT

Quy định về truy cập mạng

Truy cập dữ liệu: Chỉ được truy cập thông tin/dữ liệu được phép thông qua phân quyền

Sử dụng mạng: Không sử dụng mạng nội bộ, hệ thống thông tin, máy chủ và Internet cho mục đích ngoài công việc.

Cài đặt máy chủ: Không tự ý cài đặt các máy chủ cung cấp dịch vụ (Web, FTP, Proxy, Firewall, DC, DNS, DHCP,...).

Nghiêm cấm các hành vi sau

Vượt tường lửa: Sử dụng phần mềm để vượt qua Proxy hoặc Firewall của công ty

Mục đích cá nhân: Lợi dụng hạ tầng mạng, thiết bị và tài nguyên của Công ty và khách hàng cho mục đích ngoài công việc.

Phần mềm hacker: Sử dụng hoặc thử nghiệm bất kỳ dạng phần mềm Hacker nào trong công ty

Yêu cầu nghiệp vụ đối với kiểm soát truy cập

Thiết lập quyền truy cập

Quyền truy cập dựa trên nhu cầu nghiệp vụ và yêu cầu ATTT, đảm bảo thông tin chỉ được cấp đúng và đủ cho người sử dụng.

Rà soát định kỳ

Quyền truy cập phải được rà soát định kỳ 6 tháng/lần để đảm bảo tính phù hợp và an toàn.

Loại bỏ quyền truy cập

Quyền truy cập phải được loại bỏ khi không còn nhu cầu sử dụng để tránh rủi ro bảo mật.

Kiểm soát quyền truy cập

Dựa trên nhu cầu công việc, các trường hợp ngoại lệ cần được phê duyệt thích hợp.

Quản lý truy cập hệ ứng dụng và cơ sở dữ liệu



Phân Quyền Phù Hợp

Việc phân quyền truy cập phải phù hợp với chức năng, nhiệm vụ của người sử dụng.



Điều kiện kết nối mạng nội bộ

- Cập nhật bản vá lỗi, phần mềm tự động
- Quét virus
- Quy hoạch hạ tầng



Tài Khoản Mặc Định

Các tài khoản mặc định của nhà sản xuất phải được thay đổi hoặc xóa bỏ trước khi đưa vào sử dụng.

Quản lý truy cập người dùng



Đăng ký sử dụng

Cấp phát, thay đổi và hủy bỏ đăng ký truy cập trên tất cả các hệ thống và dịch vụ thông tin.



Định danh và xác thực

Mỗi người dùng chỉ được có một định danh duy nhất và phải có biện pháp xác thực.



Quản lý đặc quyền

Giới hạn và kiểm soát việc cấp phát và sử dụng các đặc quyền bằng văn bản hoặc biện pháp kỹ thuật.



Quản lý mật khẩu và tài khoản

Quản lý, sử dụng mật khẩu và tài khoản đảm bảo an toàn theo Quy trình quản lý truy cập

4. QUY ĐỊNH VỀ SỬ DỤNG VÀ TRUY CẬP MẠNG NỘI BỘ



Icetea Software

Trách nhiệm quản lý hệ thống CNTT

Xây dựng bảng phân quyền

Phối hợp xây dựng bảng phân quyền truy cập của từng hệ thống phần mềm nghiệp vụ.

Cài đặt hệ thống quản lý

Cài đặt các hệ thống quản lý vận hành đảm bảo thực hiện đúng theo quy định.

Rà soát tài khoản: Định kỳ 6 tháng rà soát các tài khoản không còn sử dụng để thu hồi, hủy bỏ.

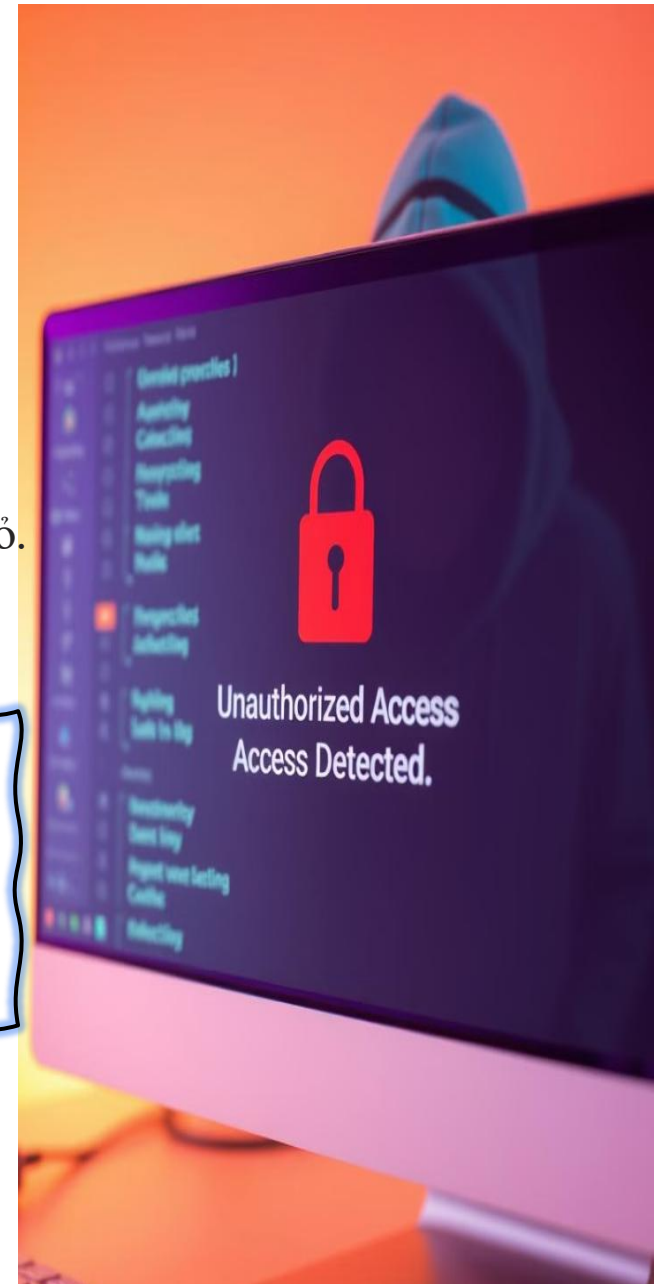
Các hành vi bị nghiêm cấm

Chỉ truy cập dữ liệu được phép thông qua phân quyền của người có thẩm quyền.

Không cho người khác mượn tài khoản hoặc để lộ mật khẩu.

Không được sử dụng mạng nội bộ để đăng tải những thông tin chống lại cá nhân, tổ chức, vi phạm thuần phong mỹ tục và quy định an ninh quốc phòng.

Không truy cập website không liên quan hoặc đã bị chặn.



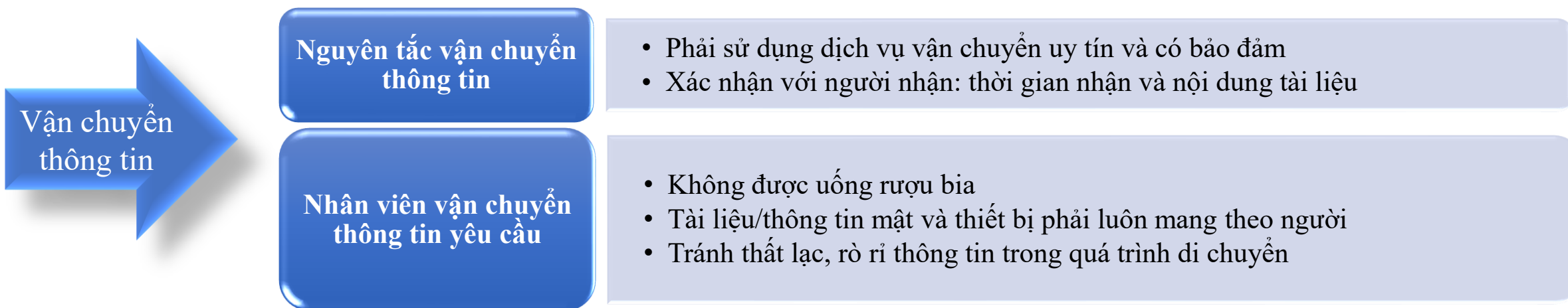
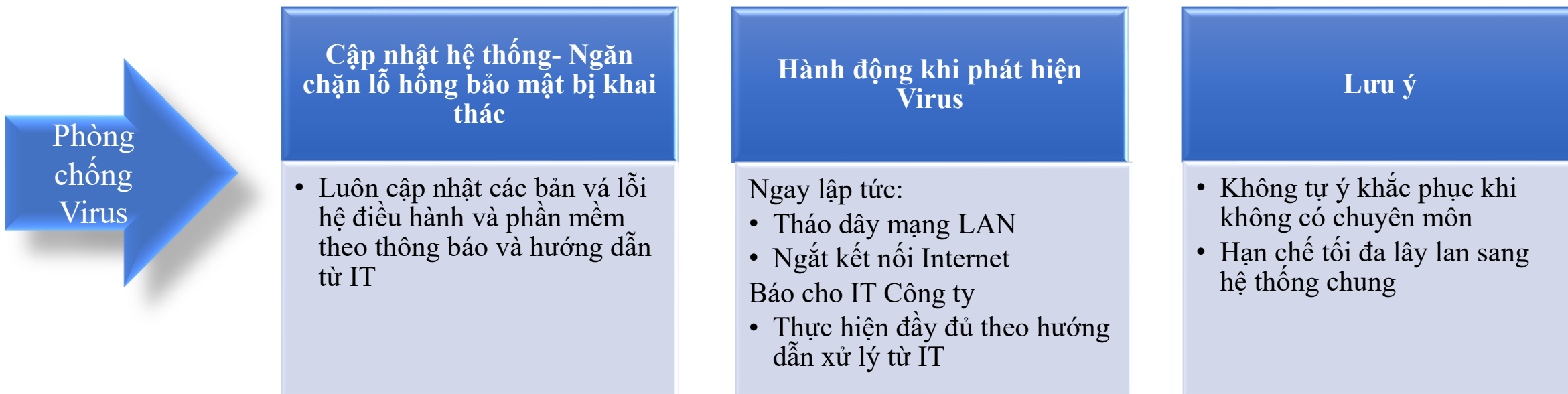
5. QUY ĐỊNH VỀ SỬ DỤNG EMAIL CÔNG TY

Mục đích quy định

- Đảm bảo **an toàn thông tin** trong hoạt động trao đổi qua email
- Bảo vệ **tài sản thông tin** của Công ty
- Giảm thiểu rủi ro rò rỉ, mất mát hoặc bị khai thác trái phép

(* Người gửi không quen, Nội dung bất thường, File hoặc link lạ, Tính cấp bách cao,...)

Email công ty	Tài khoản thông tin	Quy tắc gửi email	Các hành vi cấm khi sử dụng Email	Đăng ký không hợp lệ	Cẩn trọng email lạ (*)	Bảo vệ tài khoản email
<p>Chỉ sử dụng email do Công ty cấp hoặc email khách hàng cấp cho công việc</p> <ul style="list-style-type: none">• Cấm sử dụng email cá nhân hoặc email hệ thống không được phép tại Công ty	<ul style="list-style-type: none">• Tất cả thông tin gửi/nhận qua email Công ty đều là tài sản thông tin của Công ty• Phải bảo mật và sử dụng đúng mục đích	<ul style="list-style-type: none">• Kiểm tra kỹ: TO, CC, BCC, tiêu đề, nội dung và tệp đính kèm• File đính kèm phải: Mã hóa/đặt mật khẩu; Không gửi mật khẩu trong cùng Email	<ul style="list-style-type: none">• Email test• Sử dụng email người khác• Giả mạo, bẻ khóa, xâm nhập, tấn công• Gửi email xúc phạm, công kích, phản cảm, vi phạm luật pháp• Gửi thư rác	<ul style="list-style-type: none">• Không sử dụng email Công ty để đăng ký vào diễn đàn mạng xã hội, dịch vụ không phục vụ công việc	<ul style="list-style-type: none">• Không mở email từ địa chỉ lạ• Xóa ngay lập tức nếu nghi ngờ là email giả mạo hoặc có hại	<ul style="list-style-type: none">• Mật khẩu ít nhất 8 ký tự gồm chữ hoa, thường, số, ký tự đặc biệt• Thay đổi định kỳ: Ít nhất mỗi 90 ngày• Không chia sẻ mật khẩu, bảo mật tuyệt đối



7. QUY ĐỊNH VỀ SỬ DỤNG MÁY IN, MÁY HỦY GIẤY, TÀI LIỆU BẢN CỨNG – QUY ĐỊNH RA VÀO CÔNG TY



Icetea Software

Hủy tài liệu an toàn

- **Phải dùng máy hủy giấy** để hủy tài liệu có thông tin nhạy cảm: Hợp đồng, Bảng lương, hồ sơ dự án, báo cáo tài chính, Hồ sơ khách hàng, dự thầu, doanh thu...

Bảo vệ tài liệu bản cứng

- **Không để tài liệu Mật và Tuyệt mật** ở các khu vực công cộng: Máy in, máy photocopy, phòng họp, bàn làm việc
- **Bản cứng được lưu tại tủ có khóa và đúng vị trí quy định**

Quy định ra vào Công ty đối với nhân viên ITS

- Nhân viên công ty được phép ra vào để làm việc
- Khu vực màu vàng & đỏ: Chỉ tiếp cận trong phạm vi công việc được phân công

Quy định với khách

- Khách đến công ty cần được quản lý, đăng ký, lưu trữ thông tin với Admin và cập nhật trên <https://forms.gle/f73Ah7YUg8mmALEt6>
- Nhân viên không được tự ý mở cửa cho người lạ

Bảo vệ tài sản và kiểm soát ra vào

- Tất cả cửa ra vào phải luôn được khóa
- Nhân viên chịu trách nhiệm giải quyết hậu quả nếu không tuân thủ gây sự cố mất mát tài sản công ty.

PHÂN VÙNG ATTT

- **Khu vực màu Đỏ - mức độ Cao:**
Phòng họp khu vực BGĐ, Khu vực làm việc của BGĐ, phòng server, khu dự án quan trọng.
- **Khu vực màu Vàng - mức độ Trung bình:** Khu vực làm việc của các phòng ban tại tầng 15 và tầng 17.
- **Khu vực không gắn màu- mức độ Thấp:** Khu vực pantry, lối đi chung.





**KHU VỰC
HẠN CHẾ TIẾP CẬN
RESTRICTED AREA**



**KHU VỰC
HẠN CHẾ TIẾP CẬN
RESTRICTED AREA**

QUY ĐỊNH ATTT THEO VÙNG

- **Khu vực màu đỏ:** 
 - Cấm quay phim, chụp ảnh
 - Chỉ được tiếp cận khi có sự đồng ý của ban lãnh đạo, trưởng bộ phận và có nhân sự giám sát quá trình tiếp cận
- **Khu vực màu vàng:** 
 - Cấm quay phim, chụp ảnh
 - Chỉ được tiếp cận khi có người làm việc trong phòng
- **Khu vực thường:**
 - Được phép tiếp khách và các đối tác
 - Được phép sử dụng các thiết bị cầm tay

5. TRÁCH NHIỆM TUÂN THỦ ATTT CỦA QUẢN LÝ, NHÂN VIÊN ITS



Trách nhiệm của quản lý, nhân viên trong việc tuân thủ an toàn thông tin (ATTT) là rất quan trọng để bảo vệ dữ liệu và hệ thống thông tin của Công ty.

➤ **Tuân thủ chính sách và quy định**

Hiểu và thực hiện đúng các quy định, chính sách về ATTT của công ty.

Không được cố tình né tránh hoặc vi phạm các quy trình bảo mật.

➤ **Bảo vệ tài khoản và thiết bị**

Giữ bí mật thông tin đăng nhập, không chia sẻ tài khoản.

Khóa thiết bị khi rời khỏi chỗ làm, cập nhật phần mềm thường xuyên.

➤ **Báo cáo sự cố kịp thời**

Thông báo ngay cho bộ phận IT khi phát hiện hành vi bất thường, rò rỉ dữ liệu, email lừa đảo, mã độc...

Không tự ý xử lý nếu không có chuyên môn, tránh làm tình hình nghiêm trọng hơn.



Sự cố dẫn đến đâu?

Sự cố: Rò rỉ thông tin của Công ty, của khách hàng ra bên ngoài.

Công ty tốn thời gian công sức, tiền bạc để xử lý sự cố. Người vi phạm có các mức phạt tương ứng.

Mất lòng tin đối với khách hàng có thể dẫn đến mất hợp đồng, mất quan hệ với khách hàng.

Công ty thiệt hại lớn và phải đền bù thiệt hại cho khách hàng.

Ảnh hưởng đến uy tín, hình ảnh của công ty.



1. Thông báo ngay lập tức cho Trưởng ban ISO và các thành viên ban ISO theo Danh sách thông tin liên lạc khi xảy ra sự cố ATTT trong vòng 2h để giải quyết.
2. Các bộ phận có liên quan cần xác định **nguyên nhân**, đưa ra hành động khắc phục, phòng ngừa để tránh việc lặp lại sự cố;
3. **Mọi nhân viên** phải có **trách nhiệm** trong xử lý sự cố về ATTT;
4. Mức xử lý kỷ luật người vi phạm ATTT theo quy định tại Nội quy lao động công ty, mức kỷ luật cao nhất là **sa thải**.
5. Mức xử phạt hành chính và đền bù tổn thất sự cố theo Cam kết trong bộ NDA đã ký với với Công ty.

Danh sách thông tin liên lạc khi xảy ra sự cố ATTT

STT	Họ và tên	Chức vụ	Email	Telegram
1	Ms. Lê Thị Diệu Thúy	Trưởng ban ISO	thuyltd@iceteasoftware.com	Thuyltd
2	Mr. Nguyễn Viết Thành	Phó ban ISO	josh@iceteasoftware.com	kapparino
3	Ms. Hoàng Thị Thu Hiền	Thư ký ban ISO	hienhtt@iceteasoftware.com	hienhoang25
4	Mr. Nguyễn Bá Long	IT Help desk	longnb@iceteasoftware.com	Long160220
5	Mr. Trần Hoàng Hải	GĐ BP sản xuất GLYPH	haith@iceteasoftware.com	EricTran90
6	Mr. Phạm Hùng	GĐ BP sản xuất BLC	hungp@iceteasoftware.com	hulk_1901
7	Ms. Hứa Thị Hương	Trưởng phòng HCNS	huonght1@iceteasoftware.com	Huonght17
8	Ms. Trần Thị An	Trưởng phòng ĐBNL	antt@iceteasoftware.com	tranan198
9	Mr. Lê Xuân Tùng	GĐ BP Sale Global	tunglx@iceteasoftware.com	tunglx12
10	Ms. Nguyễn Thanh Hương	GĐ BP Sale Korea	grace@iceteasoftware.com	Grace_nguyen2210
11	Ms. Nguyễn Thị Ngọc Giang	GĐ Sale Web3	giangntn@iceteasoftware.com	olivsund
12	Mr. Vương Trọng Nhân	GĐ BP ITK	nhanvt@iceteasoftware.com	nathanvuong

XỬ LÝ VI PHẠM

Tất cả vi phạm liên quan đến an toàn thông tin đều được coi là vi phạm ở mức độ Nghiêm trọng

Yêu cầu các nhân sự ký NDA về Bảo mật an toàn thông tin khi gia nhập công ty

Trường hợp phát hiện bất kỳ sự cố vi phạm ATTT: Yêu cầu thành viên báo cáo ngay lập tức tới Quản lý trực tiếp và Thành viên ban ISO.



Question & Answer

