**QUẢN LÝ RỦI RO TRONG DOANH NGHIỆP**

**ĐỀ TÀI: Giải pháp Data Loss Prevention cho doanh nghiệp**

A picture containing game

Description automatically generated

**20522019 – Võ Thành Tín**

**20520454 – Trần Trí Đức**

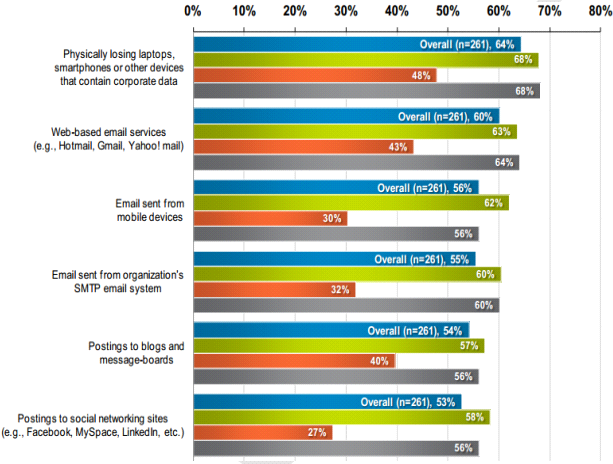
**20521291 – Huỳnh Thế Hào**

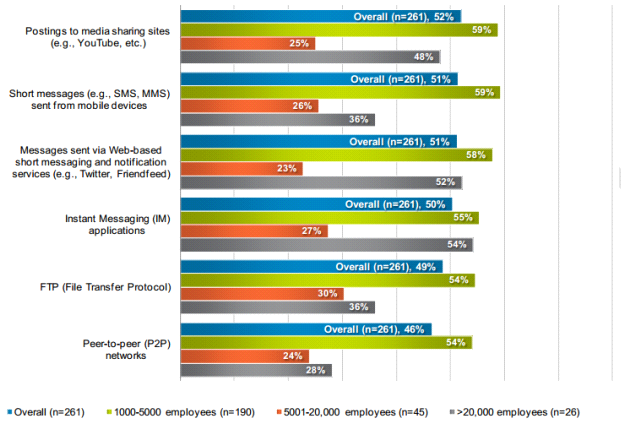
**20521858 – Nguyễn Ngọc Tài**

# MỤC LỤC

# MỤC TIÊU CỦA ĐỀ TÀI

Data Loss Prevention là một trong những mối đe dọa lớn nhất trong lĩnh vực an toàn thông tin của doanh nghiệp. Thống kê những phương thức có thể gây mất mát dữ liệu của Proofpoint vào năm 2010.



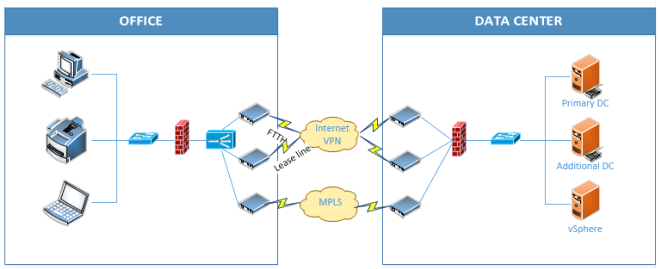


Hiện nay ở Việt Nam, vấn đề này đang được các doanh nghiệp quan tâm. Nhận thức được sức “nóng” của vấn đề này, chúng ta hãy cùng nghiên cứu và đưa ra giải pháp để khắc phục vấn đề này.

# HIỆN TRẠNG HỆ THỐNG MẠNG CỦA DOANH NGHIỆP

Hiện tại doanh nghiệp có khoảng 100 người dùng. Thông tin chi tiết các dịch vụ chạy trong hệ thống xem hình bên dưới. Những thông tin chi tiết về thống:

* Quản trị theo mô hình Domain.
* Router Cisco tích hợp Firewall.
* Thiết bị cân bằng tải kết nối internet.
* Không có phần mềm antivirus, firewall chuyên dụng cũng như các chính sách bảo mật khác.
* Chưa có hệ thống lưu trữ dữ liệu tập trung.
* Hệ thống email sử dụng hosting ngoài internet.
* Chưa có hệ thống backup dữ liệu.
* Chưa có chính sách sao lưu và phục hồi dữ liệu.
* Tất cả các máy chủ đặt tại văn phòng công ty.



Hình 1 Mô hình mạng ban đầu

# Phân tích những điểm yếu trong mô hình mạng hiện tại và rủi ro mất mát dữ liệu

## Rủi ro 1:

Hệ thống chưa có phần mềm antivirus, khả năng bị tấn công:

* Lây nhiễm virus 🡪 Bị đánh cắp dữ liệu
* Lây nhiễm ransomware 🡪 Bị mã hóa dữ liệu
* Mail chưa kiểm duyệt đến chứa nội dung không an toàn 🡪 Bị lây nhiễm malware

## Rủi ro 2:

Hệ thống chưa có thiết bị kiểm tra e-mail:

* Nội dung email độc hại 🡪 Bị lây nhiễm virus, ransomware, …
* Nhân viên tiết lộ thông tin ra mật ra ngoài 🡪 Bị rò rỉ dữ liệu
* Spam email 🡪 Nguy cơ cao tắt nghẽn dịch vụ email

## Rủi ro 3:

Chưa thiết lập mã hóa dữ liệu truyền đi:

* Gọi tin bị nghe lén 🡪 Rò rỉ dữ liệu

## Rủi ro 4:

Hệ thống chưa có cơ chế backup:

* Sự cố mất dữ liệu 🡪 Không thể khôi phục
* Thiên tai tự thiên 🡪 Mất tất cả

## Rủi ro 5:

Hệ thống chưa có phần mềm quản lý các máy nhân viên:

* Nhân viên chủ động leak thông tin 🡪 Dữ liệu bị đánh cắp
* Nhân viên để password mặc định 🡪 Dễ dàng truy cập
* Nhân viên sử dụng các phần mềm crack 🡪 Lây nhiễm mã độc
* Nhân viên chạy các ứng dụng có quyền truy cập cao 🡪 Bị leo thang đặc quyền

## Rủi ro 6:

Hệ thống không có cơ chế hạn chế tấn công từ chối dịch vụ

* Server bị đánh sập 🡪 Thiệt hại tài chính
* Không phục vụ được khách hàng 🡪 Mất khách

## Rủi ro 7:

Hệ thống không có firewall chuyên dụng:

* Tấn công vào các vị trí thiết yếu (web app, database, máy nhân viên) 🡪 Đánh cắp dữ liệu
* DDOS attack: Những dịch vụ nào public ra ngoài internet không có firewall
* Dễ bị lây nhiễm malware attack: không kiểm soát được port truy cập internet người dùng, trusted destination, download file without scan.

## Rủi ro 8:

Không cấu hình chia vlan và port mạng nội bộ chung với wifi:

* Khách xâm nhập vào mạng nội bộ 🡪 Tăng khả năng bị tấn công.

## Rủi ro 9:

Chưa có chính sách về vấn đề an toàn thông tin trong hệ thống:

* Email gửi ra không theo chính sách 🡪 Rò rỉ thông tin
* Người dùng truy cập web không theo chính sách 🡪 Đánh cắp session, dữ liệu, …
* Database xuất dữ liệu không theo chính sách 🡪 Lộ dữ liệu nhạy cảm

## Rủi ro 10:

Tất cả máy chủ đặt tại data center:

* Thiên tai 🡪 Mất sạch dữ liệu
* Sự cố tại tòa đặt data center 🡪 Mất sạch dữ liệu
* Data center bị đột nhập 🡪 Attacker tiếp cận được tất cả server

## Rủi ro 11:

Chưa có hệ thống sao lưu và khôi phục dữ liệu

* Thiên tai 🡪 Mất sạch dữ liệu
* Sự cố tại tòa đặt data center 🡪 Mất sạch dữ liệu
* Bị attacker xóa dữ liệu khi chiếm được server 🡪 Không thể khôi phục
* Nhân viên lỡ tay xóa dự liệu 🡪 Không thể khôi phục

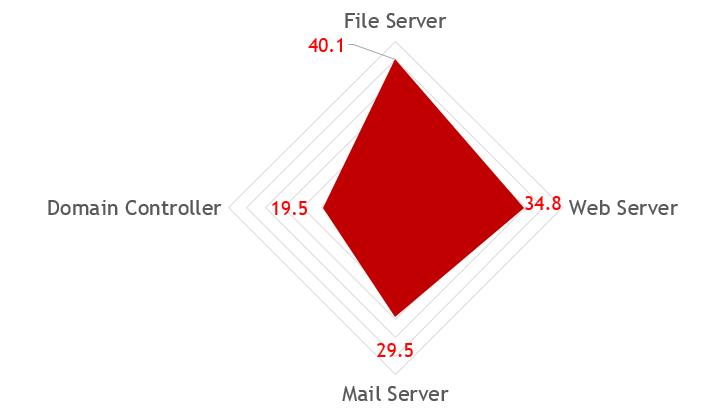
# Phân tích những rũi ro mất dữ liệu

* **Các rủi ro từ Attacker**
* Không có Firewall chuyên dụng 🡪 Dễ bị xâm nhập, gửi dữ liệu ra ngoài.
* Không có Monitoring System 🡪 Khó giám sát hệ thống.
* Dễ bị nghe lén thông tin do việc không triển khai mã hóa đường truyền tốt.
* Không có Email Security 🡪 Dễ bị Spam Mail, gửi link mã độc.
* Không có Endpoint Security 🡪 User dễ bị dính mã độc, backdoor.
* **Các rủi ro từ nhân viên**
* Không có Firewall chuyên dụng 🡪 Nhân viên có thể chuyển file thông qua Skype, Zalo, hoặc upload lên Google Drives, One Drives
* Nhân viên có thể dung các giao thức Share File P2P để chia sẻ dữ liệu
* Không có chính sách quy định về việc in ấn dữ liệu 🡪 Nhân viên có thể tận dụng lỗ hổng này để bán thông tin
* **…..**
* **…..**
* **Phân tích bao gồm các thành phần trong hệ thống như sau:**
* Web applicaion
* Domain Controller Server
* File server
* Mail service

## Ảnh hưởng (Impact)

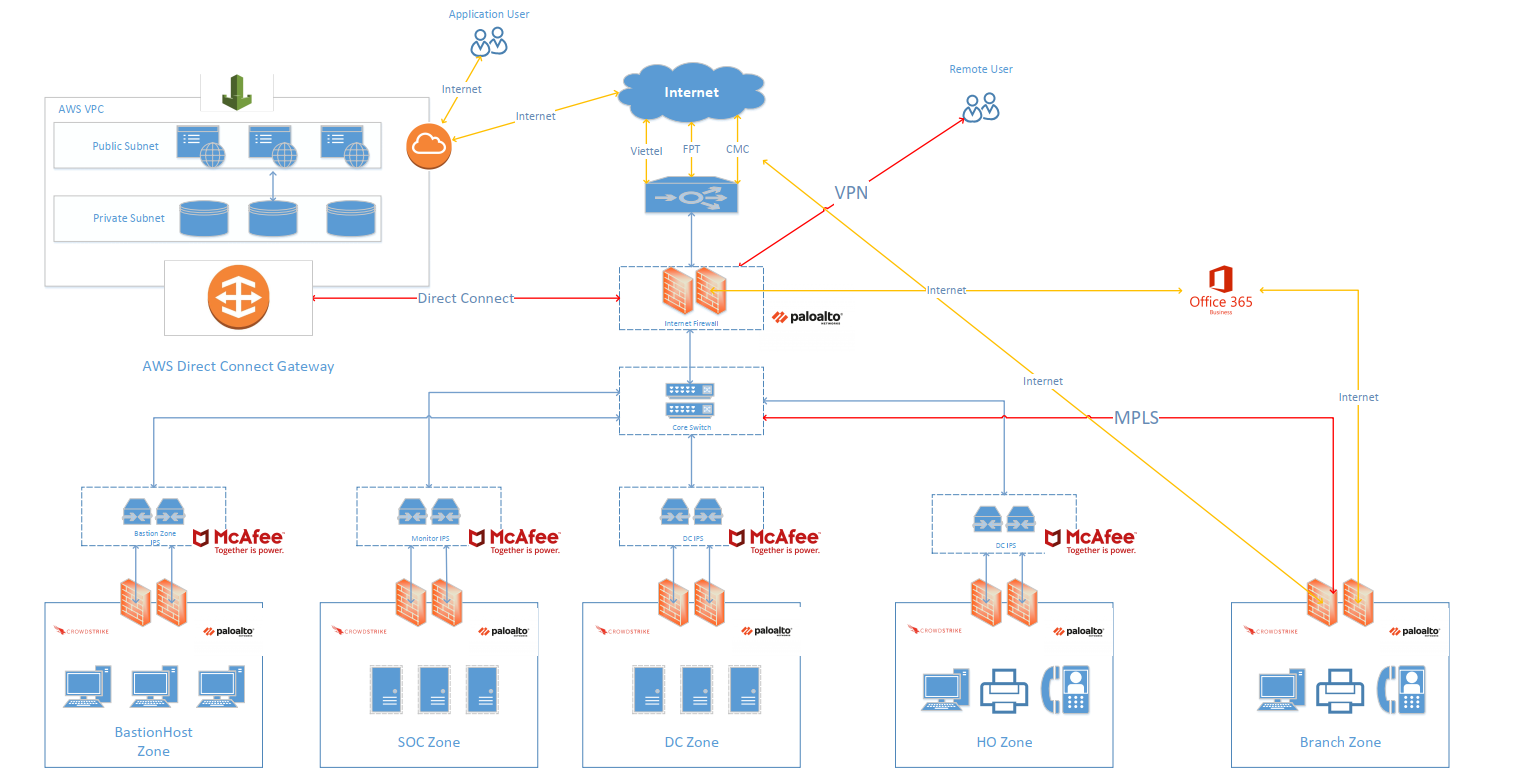
## Tần suất (Likelihood)

## Risk rank của hệ thống hiện tại



# Thiết kế lại hệ thống – mạng để giảm thiểu rủi ro mất mát dữ liệu

## Vẽ mô hình tổng thể

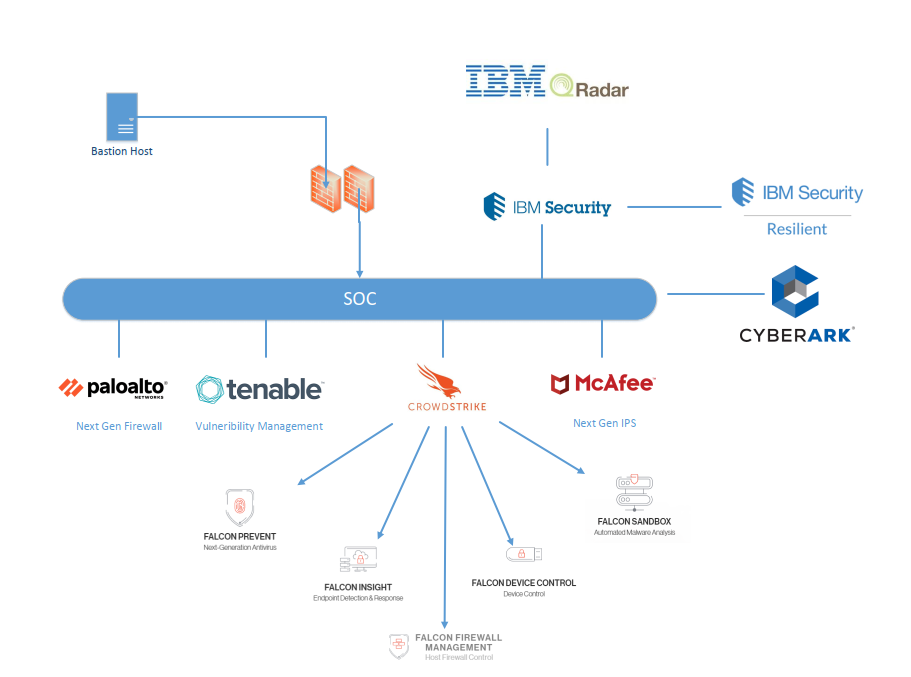


Hình 2 Mô hình mạng tổng thể

* Sơ đồ được chia làm 3 Zone chính: là SOC Zone, DC Zone, và Cloud Zone
* Có một Zone phụ là Bastion Host Zone, là Zone cho các máy tính đặc biệt, các máy tính này được ngắt kết nối hoàn toàn với Internet. Mục đích của các máy này là để quản trị viên truy cập vào các hệ thống quan trọng như DB, Server
* Còn 2 Zone phụ nữa là HO Zone (Head Office) và Branch Zone (Chi nhánh). HO Zone được đặt tại DC nên không lo về kết nối. Branch Zone là các chi nhánh sẽ đi Internet bình thường. Khi có nhu cầu truy cập về File Server thì sẽ đi thông qua MPLS về Data Center.
* Ở đây nhóm sử dụng Office 365 để làm Mail cho nhân viên, sử dụng hệ thống ngăn chặn Mail Spam của Office 365.

## Mô hình chi tiết

### Mô hình SOC Zone (Security Operations Center Zone)

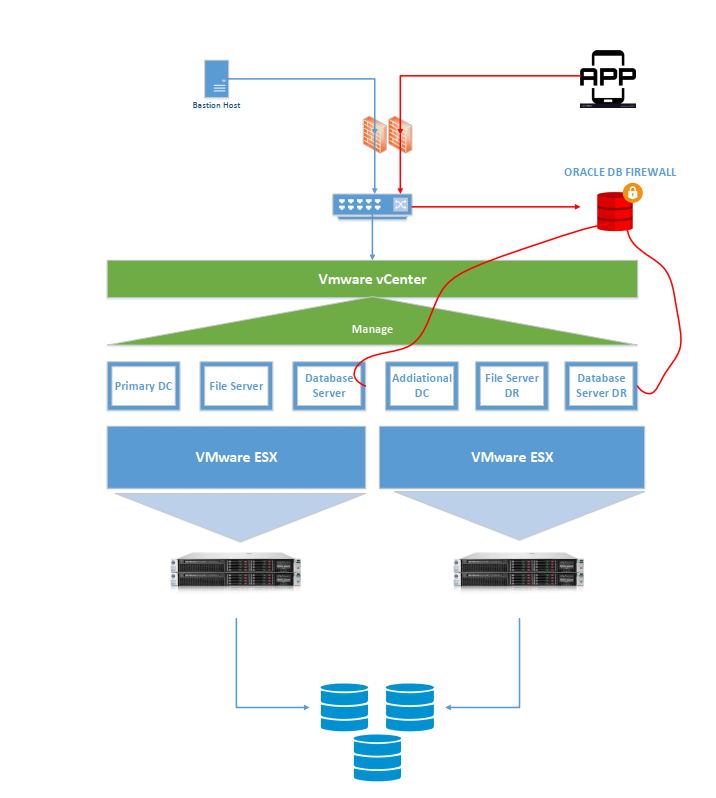


Hình 3 Mô hình SOC Zone

SOC Zone là bộ não vận hành bảo mật cho hệ thống. Nhóm sử dụng các thành phần sau:

* Palo Alto Firewall: Tường lửa thế hệ mới
* Tenable: giải pháp Vulnerability Management để kiểm soát lỗ hổng của hệ thống
* McAfee IPS: Giải pháp ngăn ngừa xâm nhập của McAfee
* Crowdstrike: Hệ thống Endpoint, Sandbox và DLP của Crowdstrike
* IBM: Sử dụng SIEM và SOAR của IBM.
* CyberArk: Privilege Access Management, dùng để quản lý quyền truy cập của các tài khoản đặc quyền.

### Mô hình DC Zone (Data Center Zone)

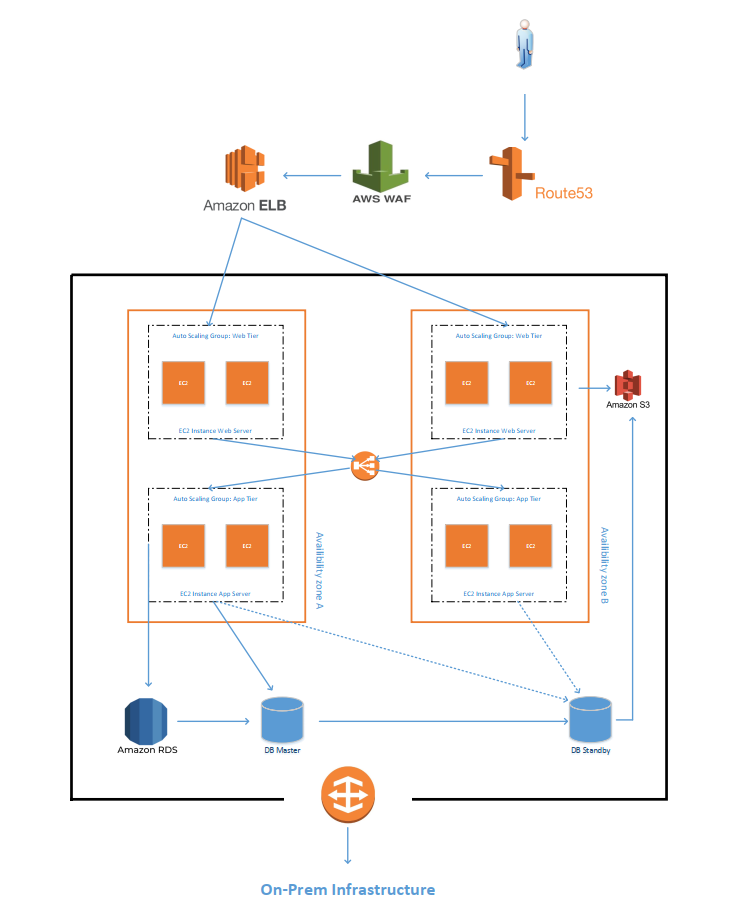


Mô hình DC Zone

DC Zone nhóm sử dụng Vmware vSphere như hình trên

* Các máy chủ được cài đặt Vmware OS
* Sử dụng giải pháp Backup của SAN

### Cloud Zone



Cloud Zone được kết nối về Data Center (On Prem) thông qua AWS Direct Connect

* Trong Cloud Zone chủ yếu là các ứng dụng Web
* Hệ thống Cloud này được chia ra thành 2 Availibility Zone (AZ)
* Thực hiện cân bằng tải giữa 2 AZ.
* Hệ thống Web trên Cloud này được phân quyền truy cập từ bên ngoài dựa vào Security Group
* Thực hiện Backup DB bằng S3, Backup máy chủ bằng cơ chế Snapshot
* Sử dụng AWS WAF để ngăn chặn việc tấn công vào Web

# Xây dựng quy trình và chính sách để phối hợp với các công nghệ sử dụng trong hệ thống để giảm mất mát dữ liệu trong hệ thống

## Chính sách bảo mật máy chủ

* **Quy định chung**

1. Tất cả các máy chủ nội bộ được triển khai tại công ty phải thuộc sở hữu của một nhóm hoạt động gồm những người chịu trách nhiệm quản lý hệ thống. Hướng dẫn cấu hình máy chủ hợp lệ phải được thiết lập và duy trì bởi mỗi nhóm hoạt động, dựa trên nhu cầu kinh doanh và được thông qua bởi InfoSec. Các nhóm hoạt động nên theo dõi việc tuân thủ cấu hình và thực hiện chính sách ngoại lệ phù hợp với môi trường của họ. Mỗi nhóm hoạt động phải thiết lập một quy trình để thay đổi hướng dẫn cấu hình, bao gồm việc xem xét và thông qua bởi bộ phận IT. Cần phải thỏa một số yêu cầu dưới đây:

Các máy chủ phải được đăng ký trong hệ thống quản lý doanh nghiệp của công ty. Ít nhất, cần có các thông tin sau đây để xác định rõ hướng liên lạc:

* Server contact(s), location, backup contact.
* Hardware và Operating System/Version
* Main functions, applications, …

Thông tin trong hệ thống quản lý doanh nghiệp doanh nghiệp phải được cập nhật mới nhất.

Các thay đổi về cấu hình cho các máy chủ sản xuất phải tuân thủ các quy trình quản lý thay đổi thích hợp.

2. Cho mục đích bảo mật, tuân thủ, và bảo trì, nhân viên có quyền hạn có thể giám sát và kiểm toán các trang thiết bị, hệ thống, quy trình và lưu lượng mạng dựa trên Chính sách Kiểm toán.

* **Yêu cầu cấu hình**

1. Để đảm bảo an toàn, tuân thủ và duy trì mục tiêu, nhân viên được ủy quyền có thể theo dõi và kiểm tra thiết bị, hệ thống, quy trình và lưu lượng mạng theo Chính sách Kiểm toán.

2. Các dịch vụ và ứng dụng sẽ không được sử dụng phải được vô hiệu hóa ở nơi thực thi.

3. Truy cập vào các dịch vụ cần được ghi lại hoặc bảo vệ thông qua các phương pháp kiểm soát truy cập như firewall, ứng dụng web, …

4. Các bản vá lỗi bảo mật mới nhất phải được cài đặt trên hệ thống ngay khi được công bố, ngoại lệ duy nhất là khi thay đổi ứng dụng ngay lập tức sẽ cản trở các yêu cầu kinh doanh.

5. Các mối quan hệ giữa các hệ thống cũng là một nguy cơ bảo mật, vì vậy nên hạn chế việc sử dụng chúng. Không sử dụng thêm mối quan hệ tin cậy nào nếu đã có một số phương pháp truyền thông khác.

6. Luôn luôn sử dụng các chuẩn bảo mật về yêu cầu truy cập ít nhất là để thực hiện một chức năng nào đó. Không sử dụng quyền root khi một tài khoản không đủ đặc quyền thực thi.

7. Nếu có phương pháp kết channel an toàn (khả thi về mặt kỹ thuật), quyền truy cập có đặc quyền phải được thực hiện qua các kênh truyền an toàn, (ví dụ: các kết nối mạng được mã hóa sử dụng SSH hoặc IPSec).

8. Các máy chủ phải được đặt trong một môi trường được kiểm soát truy cập.

9. Các máy chủ đặc biệt bị cấm vận hành từ các khu vực phòng không kiểm soát được.

* **Giám sát**

1. Tất cả các sự kiện liên quan đến an ninh trên các hệ thống quan trọng hoặc nhạy cảm phải được đăng nhập và kiểm tra con đường được lưu như sau:

* Tất cả bản ghi liên quan đến bảo mật sẽ được giữ trực tuyến tối thiểu là 1 tuần.
* Các bản sao lưu hàng ngày sẽ được giữ lại trong ít nhất 1 tháng.
* Các bản sao lưu toàn bộ log hàng tuần sẽ được giữ lại trong ít nhất 1 tháng.
* Sao lưu toàn bộ hàng tháng sẽ được giữ lại trong tối thiểu 2 năm.

2. Các sự kiện liên quan đến vấn bảo mật sẽ được báo cáo với bộ phận IT - người sẽ xem xét log và các báo cáo sự cố cho phòng quản lý CNTT. Các biện pháp khắc phục sẽ được quy định khi cần; các sự kiện liên quan đến bảo mật bao gồm nhưng không giới hạn bởi những điều dưới đây:

* Tấn công quét port.
* Bằng chứng về việc truy cập trái phép vào các tài khoản đặc quyền.
* Sự xuất hiện bất thường nhưng không liên quan đến các ứng dụng cụ thể nào trên máy chủ.
* **Tuân thủ chính sách**

Bộ phận IT sẽ xác minh việc tuân thủ chính sách này thông qua các phương pháp khác nhau, bao gồm nhưng không giới hạn bởi periodic walk-thrus, video monitoring, business tool reports, kiểm toán nội bộ và bên ngoài, phản hồi cho chủ sở hữu chính sách.

Bất kỳ trường hợp ngoại lệ nào đối với chính sách phải được trưởng bộ phận IT hoặc Tổng giám đốc chấp thuận trước.

Nếu nhân viên vi phạm chính sách này có thể bị kỷ luật, kể cả việc chấm dứt hợp đồng lao động.

* **Tiêu chuẩn, chính sách liên quan**

Chính sách Kiểm toán.

## Quản lý khôi phục và sao lưu cơ sở dữ liệu

* **Chính sách sao lưu dữ liệu**

1. Full backups được thực hiện hàng tuần và được lưu trữ trong 3 tháng trước khi bị ghi đè.

2. Phần dữ liệu mới được backup vào DC side hàng ngày và được lưu trữ trong 1 tháng trước khi bị ghi đè.

3. Việc backup sang DR side được thực hiện từ 01:00 am đến trước 9:00 am cùng ngày.

4. Sau khi hoàn thành quá trình sao lưu, các bản sao của phương tiện truyền thông sẽ tự động di chuyển đến một nơi an toàn từ xa để phục hồi sau thảm họa.

5. Các bản sao lưu được lưu trữ ở các vị trí an toàn. Chỉ một số nhân viên được ủy quyền mới có quyền truy cập vào các ứng dụng sao lưu và bản sao phương tiện truyền thông.

6. Yêu cầu sao lưu dữ liệu từ bên thứ ba phải được Giám đốc chấp thuận.

* **Chính sách khôi phục dữ liệu**

1. Dữ liệu có sẵn để phục hồi trong vòng vài phút nếu thực hiện khôi phục dữ liệu ngày.

2. Dữ liệu sẽ có trong chính sách lưu giữ của mỗi công việc sao lưu - hiện được xác định là 3 tháng.

3. Dữ liệu gần đây có sẵn từ hệ thống khi hoàn thành công việc sao lưu hàng ngày, có nghĩa là dữ liệu có thể bị mất trong một ngày làm việc trên một số hệ thống.

4. Yêu cầu phục hồi dữ liệu phải được gửi tới bàn bộ phận IT.

* **Tuân thủ chính sách**

Bộ phận IT sẽ xác minh sự tuân thủ chính sách này thông qua nhiều cách khác nhau, bao gồm không giới hạn, kiểm tra đột xuất, giám sát video, báo cáo công cụ kinh doanh, kiểm toán nội bộ và bên ngoài, và sẽ cung cấp phản hồi cho chủ sở hữu chính sách và doanh nghiệp thích hợp đơn vị quản lý.

Bất kỳ nhân viên nào vi phạm sẽ bị xử phạt tùy mức độ, có thể dẫn đến thôi việc.

## Chính sách sử dụng thiết bị lưu trữ gắn ngoài

1. Không sử dụng thiết bị gắn ngoài để sao chép dữ liệu ra khỏi máy tính và server của công ty khi chưa được sự đồng ý của IT Manager.

2. IT Manager được toàn quyền quyết định việc cho phép sử dụng thiết bị lưu trữ gắn ngoài đối với từng trường hợp. Lúc đó phải có biên bản ghi cụ thể thời gian mở khoá và khoá thiết bị.

3. Toàn bộ dữ liệu khi được sao chép phải được mã hoá tự động bằng Kaspersky Endpoint Security.

4. Dữ liệu được chép vào thiết bị lưu trữ gắn ngoài sẽ được ghi log tự động và gửi về máy chủ quản lý. IT Manager không được phép biết nội dung và mật khẩu của các file này.

5. Dữ liệu từ thiết bị lưu trữ gắn ngoài không thể chép vào trong máy tính và server của công ty. Chỉ có những thiết bị riêng của bộ phận IT mới được sử dụng với mục đích cài đặt mới máy tính.

6. Dữ liệu trong thiết bị gắn ngoài có liên quan đến công ty do người ký văn bản xin phép sử dụng chịu hoàn toàn trách nhiệm nếu có mất mác xảy ra.

7. Đối với nhân viên vệ sinh, nhân viên bảo vệ và nhân viên phòng kế toán không được phép sử dụng thiết bị gắn ngoài khi vào nơi làm việc.

8. Nhân viên phòng IT chỉ được sử dụng thiết bị gắn ngoài của công ty cung cấp. Không được tự ý đem thiết bị lạ vào văn phòng.

* **Tuân thủ chính sách**

Việc kiểm soát thực hiện chính sách này hoàn toàn do phòng IT Manager thực hiện.

Các trường hợp thất thoát dữ liệu, Trưởng IT Manager sẽ chịu trách nhiệm rà soát và điều tra dưới sự giám sát của Giám đốc điều hành.

Các hành vi qua mặt phần mềm, phần cứng để sao chép tài liệu vào thiết bị lưu trữ gắn ngoài sẽ bị xử lý từ hạ bậc hiệu suất làm việc trong năm đến xử lý Hình sự (trong trường hợp mất tài sản tối quan trọng ảnh hưởng nghiêm trọng đến công ty).

Các trường hợp ngoại lệ sẽ được quyết định bởi IT manager – Có biên bản kèm theo.

## Chính sách email

### Tổng quan

Thư điện tử được sử dụng rộng rãi trong hầu hết các lĩnh vực ngành nghề, thường được dùng trong giao tiếp/hội thoại và nhận thức chính trong một tổ chức. Đồng thời, lạm dụng sử dụng email có thể làm tăng nhiều rủi ro về pháp lý, bảo mật và an ninh. Do đó, cần phải người dùng phải hiểu được cách sử dụng truyền thông điện tử thích hợp.

### Mục đích

Mục đích của chính sách email là để đảm bảo sử dụng hệ thống email phù hợp, làm cho người dùng có thể nhận thức được hành động được chấp nhận và không chấp nhận của hệ thống email. Policy này đề ra những yêu cầu tối thiểu cho việc sử dụng email trong môi trường mạng.

### Phạm vi

Chính sách này thích hợp để áp dụng cho việc sử dụng bất kỳ email nào được gửi từ địa chỉ email của công ty và áp dụng cho tất cả nhân viên, nhà cung cấp và đại lý hoạt động thay mặt cho công ty.

### Chính sách

1. Tất cả việc sử dụng email phải phù hợp với chính sách và hành vi đạo đức, an toàn, tuân thủ pháp luật và thực tiễn kinh doanh phù hợp.

2. Tài khoản email nên được sử dụng chủ yếu cho các mục đích kinh doanh; giao tiếp cá nhân vẫn được cho phép nhưng có giới hạn, ngoài ra việc sử dụng cho mục đích thương mại không liên quan đều bị cấm.

3. Tất cả dữ liệu chứa trong email hoặc tệp đính kèm phải được bảo mật theo Tiêu chuẩn Bảo vệ Dữ liệu.

4. Email chỉ nên được giữ lại nếu nó đủ điều kiện làm hồ sơ kinh doanh. Email là một bản ghi kinh doanh nếu hợp pháp và doanh nghiệp vẫn đang hoạt động, mục đích để bảo vệ, giữ gìn thông tin chứa trong email.

5. Email được xác định là hồ sơ kinh doanh sẽ được giữ lại theo Record Retention Schedule.

6. Hệ thống email sẽ không được sử dụng cho việc tạo ra hoặc phân phối bất kỳ tin nhắn phá hoại hoặc gây xúc phạm nào, bao gồm các ý kiến xúc phạm về chủng tộc, giới tính, màu tóc, khuyết tật, tuổi tác, khuynh hướng tình dục, khiêu dâm, tín ngưỡng và tôn giáo, chính trị, nguồn gốc quốc gia. Nhân viên nhận được bất kỳ email có nội dung này từ bất kỳ nhân viên nào nên báo cáo cho người giám sát của họ ngay lập tức.

7. Người dùng bị cấm tự động chuyển tiếp email đến hệ thống email của bên thứ ba (lưu ý trong ý 8 dưới đây). Các tin nhắn riêng lẻ được chuyển tiếp bởi người sử dụng không được chứa thông tin bí mật hoặc ở trên.

8. Người dùng bị cấm sử dụng các hệ thống email của bên thứ ba và các máy chủ lưu trữ như Google, Yahoo, MSN Hotmail, ..v.v.. để tiến hành kinh doanh, tạo ra hoặc ghi nhớ bất kỳ giao dịch ràng buộc nào, lưu trữ hoặc giữ lại email thay mặt cho công ty. Các giao tiếp và giao dịch như vậy phải được thực hiện thông qua các kênh phù hợp, sử dụng tài liệu đã được phê duyệt.

9. Sử dụng một lượng tài nguyên hợp lý cho email cá nhân là chấp nhận được, nhưng email không liên quan đến công việc sẽ được lưu trong một thư mục riêng biệt, cách biệt với email liên quan đến công việc. Hành vi gửi thư dây chuyền hoặc email từ tài khoản email là bị cấm.

10. Nhân viên không nên có kỳ vọng về sự riêng tư trong bất cứ điều gì họ lưu trữ, gửi hoặc nhận trên hệ thống email của công ty.

11. Công ty có thể theo dõi tin nhắn mà không cần báo trước, không bắt buộc phải theo dõi thư điện tử.

* **Tuân thủ chính sách**

Bộ phận IT sẽ xác nhận sự tuân thủ đối với bộ luật này thông qua nhiều phương thức, không bị giới hạn, periodic walk-thrus, video monitoring, business tool reports, internal và external audits, gửi feedback đến policy owner.

Bất kì ngoại lệ nào ngoài những điều đã được quy định trong bộ luật đều cần có sự cho phép của Tổng giám đốc.

Các nhân viên vi phạm bộ luật hoặc không tuân thủ có thể bị kỷ luật, kể cả việc chấm dứt hợp đồng việc làm.

* **Tiêu chuẩn, chính sách liên quan**

Record Retention Schedule

Tiêu chuẩn Bảo vệ Dữ liệu

## Chính sách quản lý truy cập mạng

* **Kết nối mạng vật lý**

Tất cả kết nối Internet vật lý hoặc kết nối với các private network cần được ủy quyền và phê duyệt bởi phòng CNTT. Hầu hết người dùng sẽ truy cập internet thông qua các kết nối cung cấp riêng cho văn phòng của họ do bộ phận CNTT. Bất kỳ kết nối bổ sung nào cũng phải được phòng IT phê duyệt. Những kết nối bổ sung có thể ngoại lệ, không chỉ bao gồm những điều sau:

* Modem connection từ một máy tính hoặc một thiết bị giao tiếp có thể cho phép mở một kết nối đến mạng.
* Bất kỳ máy in đa năng hay máy FAX nào có cả chức năng điện thoại và kết nối mạng đều phải được kiểm tra và phê duyệt trước khi sử dụng bởi bộ phận CNTT.
* Các wireless access points hoặc các thiết bị có tính năng kết nối không dây thì không được sử dụng trước khi được phê duyệt bởi bộ phận CNTT. Nếu bất kỳ máy tính hoặc các thiết bị khác có khả năng kết nối không dây buộc phải tắt chức năng đó trước khi tự động kết nối với mạng công ty, trừ trường hợp nó được bộ phận CNTT phê duyệt cho kết nối mạng.

Bất kỳ kết nối internet bổ sung nào không do phòng CNTT cung cấp phải được xem trước và phê duyệt bởi phòng IT. Thông thường bất kỳ kết nối bổ sung từ mạng lưới công ty đến Internet hoặc private network yêu cầu:

* Một bộ phận CNTT luôn luôn trực để phê duyệt tường lửa hoạt động và cấu hình đúng.
* Một số cuộc hội thoại thông qua kết nối có thể yêu cầu mã hóa khi muốn đọc lại dữ liệu được truyền bởi bộ phận CNTT.
* **Sử dụng mạng**

Tất cả nhân viên chỉ sử dụng Internet nhằm mục đích kinh doanh.

Việc sử dụng Internet của nhân viên có thể được theo dõi và ghi lại, bao gồm thông tin tất cả các trang web được truy cập, thời gian truy cập, lượng dữ liệu đã tải về, và các loại dữ liệu đã tải về. Thời gian hoạt động cũng có thể được ghi lại.

Khuyến khích nhân viên thận trọng khi truy cập các trang web không xác định, đào tạo người dùng, giữ trình duyệt của họ được định cấu hình theo tiêu chuẩn IT được phê duyệt để bảo vệ chống lại sự nhiễm trùng phần mềm độc hại. Nhân viên sẽ được đào tạo về các tiêu chuẩn IT được phê duyệt mới nhất để bảo vệ chống lại phần mềm độc hại khi thích hợp.

* **Điều khiển truy cập mạng và hệ thống log**

Một hệ thống được đưa vào vận hành trên mạng với các khả năng sau:

* Ngăn người dùng truy cập các trang web không phù hợp, khiêu dâm, hoặc nguy hiểm. Cơ sở dữ liệu của các trang web được phân loại cập nhật thường xuyên.
* Log lại hoạt động trên internet của user:
* Thời gian hoạt động trên internet.
* Thời gian của từng hoạt động.
* Trang web đã truy cập.
* Dữ liệu và loại dữ liệu đã tải về.
* Cần có một proxy server để lưu cache của trang web nhằm tăng tốc độ truy cập.

Hệ thống có thể hoặc không yêu cầu một ID để đăng nhập, hoặc nó sẽ dùng network hiện tại để login xác thực người dùng.

Hệ thống này được sử dụng để ngăn người dùng truy cập các trang web không phù hợp, khiêu dâm, hoặc nguy hiểm. Hệ thống tương tự này sẽ không yêu cầu ID đăng nhập bổ sung và sẽ sử dụng Active Directory để xác định người dùng internet; có thể ghi lại thời gian hoạt động trên mạng, thời gian hoạt động, trang web đã truy cập, bất kỳ dữ liệu nào đã tải về và loại dữ liệu đã tải về; cache các trang web.

* **Tuân thủ chính sách**

Bất kì ngoại lệ nào ngoài những điều đã được quy định trong bộ luật đều cần có sự cho phép của phòng IT.

Việc sử dụng mobile, computers không đúng cách có thể mang lại các phần mềm gây hại, có thể phá hủy tính toàn vẹn của các tài nguyên và hệ thống mạng. Việc ngăn ngừa những sự kiện này là rất quan trọng đối với sự an toàn của tổ chức. Tất cả cá nhân, nhân viên không tuân thủ chính sách sẽ bị kỷ luật và bao gồm việc sa thải.

## Chính sách truy cập mạng nội bộ từ xa

1. Kênh truy cập từ xa phải được bảo vệ bởi cơ chế mã hóa (ví dụ: VPNs) và mật khẩu mạnh.

2. Khi kết nối đến mạng nội bộ của công ty, máy tính điều khiển không được kết nối vào bất cứ mạng nào khác ngoài mạng cá nhân mà người kết nối hoàn toàn kiểm soát.

3. Các thiết bị dùng để kết nối đến mạng nội bộ phải thỏa chuẩn điều kiện về phần cứng và phần mềm để truy cập từ xa.

* **Tuân thủ chính sách**

Bộ phận IT sẽ xác minh sự tuân thủ chính sách này thông qua nhiều cách khác nhau, bao gồm không giới hạn, kiểm tra đột xuất, giám sát video, báo cáo công cụ kinh doanh, kiểm toán nội bộ và bên ngoài và sẽ cung cấp phản hồi cho chủ sở hữu chính sách và doanh nghiệp thích hợp quản lý đơn vị.

Bất kì nhân viên nào vi phạm sẽ bị xử phạt tùy mức độ, có thể dẫn đến thôi việc.

## Chính sách bảo mật mật khẩu

* **Tạo mật khẩu**

1. Tất cả mật khẩu cấp người dùng và cấp hệ thống phải phù hợp với Hướng dẫn Xây dựng mật khẩu.

2. Người dùng không được sử dụng cùng một mật khẩu cho tài khoản công ty cũng như quyền truy cập khác của công ty khác (ví dụ như tài khoản ISP cá nhân, kinh doanh, …)

3. Khi có thể, người dùng không được sử dụng cùng một mật khẩu cho các nhu cầu truy cập khác của công ty.

4. Các tài khoản người dùng có các đặc quyền cấp hệ thống được cấp thông qua các thành viên trong nhóm hoặc các chương trình như sudo phải có một mật khẩu duy nhất từ tất cả các tài khoản khác được giữ bởi người dùng đó để truy cập các đặc quyền cấp hệ thống.

* **Đổi mật khẩu**

1. Tất cả các mật khẩu cấp hệ thống (như quyền root, NT admin, admin của ứng dụng, …) phải được đổi ít nhất mỗi quý một lần.

2. Tất cả mật khẩu cấp người dùng (như email, web, máy tính, …) phải được đổi ít nhất 6 tháng 1 lần, tốt nhất là 4 tháng 1 lần.

3. Việc lấy mật khẩu hoặc đoán mật khẩu có thể được thực hiện kiểm tra định kỳ hoặc ngẫu nhiên. Nếu mật khẩu được đoán hoặc bị phát hiện trong quá trình quét thì người dùng phải đổi mật khẩu ngay theo hướng dẫn Xây dựng mật khẩu.

* **Bảo vệ mật khẩu**

1. Mật khẩu không được chia sẻ với bất kỳ ai. Tất cả mật khẩu được coi là nhạy cảm, thông tin bí mật của công ty.

2. Mật khẩu không được đưa vào thư điện tử, hoặc các hình thức truyền thông điện tử khác.

3. Mật khẩu không được tiết lộ qua điện thoại cho bất cứ ai.

4. Không gợi ý theo định dạng của một mật khẩu.

5. Không chia sẻ mật khẩu công ty với bất kỳ ai, bao gồm cả trợ lý hành chính, thư ký, người quản lý, đồng nghiệp và các thành viên trong gia đình.

6. Không viết mật khẩu và lưu trữ chúng ở bất cứ đâu trong văn phòng của bạn. Không lưu trữ mật khẩu trong một tệp trên hệ thống máy tính hoặc thiết bị di động (điện thoại, máy tính bảng) mà không có mã hóa.

7. Không sử dụng tính năng ghi nhớ mật khẩu của ứng dụng (ví dụ: trình duyệt web).

Bất kỳ người dùng nghi ngờ rằng mật khẩu của họ có thể đã bị rò rỉ phải báo cáo vụ việc và thay đổi tất cả mật khẩu.

* **Phát triển ứng dụng**

Người phát triển ứng dụng phải đảm bảo chương trình của họ bao gồm các đề phòng bảo mật sau:

1. Ứng dụng phải hỗ trợ xác thực người dùng (cá nhân).

2. Ứng dụng không được lưu mật khẩu ở dạng bảng rõ hoặc dễ đoán mật khẩu.

3. Ứng dụng không được truyền mật khẩu ở dạng bảng rõ qua mạng.

4. Ứng dụng phải cung cấp nhiều mức độ quản lý ứng dụng theo vai trò.

* **Sử dụng mật khẩu**

Mật khẩu được sử dụng cho việc xác thực khóa công khai/khóa cá nhân. Hệ thống khóa công khai/khóa cá nhân xác định mối quan hệ toán học giữa khóa công khai mà tất cả người dùng biết và khóa riêng, chỉ người dùng biết. Nếu không có mật khẩu mở khóa cá nhân, người dùng không thể truy cập được.

Mật khẩu phải tương đối dài và chứa một sự kết hợp giữa chữ hoa, chữ thường và các ký tự số, chấm câu.

Ví dụ: "The \*? #> \* @ TrafficOnThe101Was \* & #! # ThisMorning"

* **Tuân thủ chính sách**

Bộ phận IT sẽ giám sát và xác minh sự tuân thủ chính sách này bằng các phương pháp khác nhau như theo dõi định kỳ, kiếm toán nội bộ, …

Bất kỳ ngoại lệ của chính sách phải được sự chấp thuận của trưởng bộ phận IT và tổng giám đốc.

Nhân viên vi phạm chính sách này sẽ có thể bị kỷ luật tùy theo mức độ.

* **Tiêu chuẩn, chính sách liên quan**

Hướng dẫn Xây dựng mật khẩu.

## Chính sách an ninh vật lý

* **Hệ thống báo động an ninh**

Một hệ thống bảo động an ninh phải được đặt đúng chỗ, hoạt động ở tất cả các thời điểm thích hợp như giám sát cần thiết, có dây và không dây (nếu cần) cho tất cả các điểm vào và ra trên toàn bộ cơ sở và các khu vực dễ bị tổn thương. Ngoài ra, các dịch vụ phản hồi và giải quyết cho báo động an ninh là một công cảnh báo an ninh bên thứ ba được cấp phép, có đảm bảo và có bảo hiểm hoặc cảnh sát khu vực. Hơn nữa, một bên thích hợp tại công ty sẽ được thông báo ngay lập tức và bất cứ lúc nào báo động vượt qua ngưỡng tối đa, các công ty bên thứ ba sẽ được liên lạc.

* **Sử dụng các biện pháp kiểm soát nhập cảnh phù hợp để giới hạn và giám sát truy cập vật lý vào các hệ thống lưu trữ, xử lý hoặc chuyển dữ liệu**

Tại công ty, nhân viên có quyền truy cập vào dữ liệu của mình tách biệt với các nhân viên khác và yêu cầu quyền truy cập vào khu vực làm việc của họ.

Tại data center, việc truy cập vào các thiết bị của công ty được giới hạn cho các cá nhân có quyền truy cập được ủy quyền và được giám sát thông qua camera và sử dụng máy biometric.

* **Camera/theo dõi/giám sát/ghi âm/lưu trữ**

Camera sẽ được đặt tại các vị trí cần thiết và có khả năng ghi lại tất cả các hoạt động. Ngoài ra, chỉ có nhân viên có thẩm quyền mới có thể xem lại tất cả các hoạt động được ghi lại đó. Trong giờ làm việc hoặc ngoài giờ làm việc, camera vẫn hoạt động và ghi lại tất cả các hoạt động. Hơn nữa, biện pháp lưu trữ phải được thực hiện (tối thiểu là 90 ngày) để lưu giữ dữ liệu được ghi lại trên camera.

* **Chính sách về điều kiện đe dọa**

Trong trường hợp có các trường hợp sau xảy ra cần có giải pháp, chính sách dự trù để giảm thiểu tối đa chi phí thiệt hại cho công ty:

* Đe dọa về khủng bố hoặc con tin.
* Điều kiện môi trường vật lý như động đất, núi lửa, lũ lụt, …
* Mất điện, vấn đề về các tiện ích.
* Mối đe dọa về công nghệ và sự tổn thương về dữ liệu như tấn công từ chối dịch vụ (DDoS), …
* **Nhận dạng kẻ xấu/kiểm tra thiết bị**

Bất kỳ một ai vào và ra khỏi công ty cũng cần phải được kiểm tra. Nhân viên khi vào văn phòng công ty cần có thẻ nhân viên, khách cũng có thẻ của khách, … được kiểm soát bởi bảo vệ và hệ thống quẹt thẻ. Tài sản mà những người ra và vào văn phòng công ty mang theo cũng được giám sát, kiểm tra nghiêm ngặt bởi bảo vệ để tránh việc mất cắp tài sản.

* **Tuân thủ chính sách**

Hoạt động giám sát việc tuân thủ chính sách sẽ được thực hiện định kỳ hằng quý và dưới sự quản lý của bộ phận có thẩm quyền liên quan như IT, bảo vệ, tổng giám đốc, …

Tất cả các yêu cầu ngoài những quy định trên sẽ phải được kiểm tra, đánh giá và được sự chấp thuận của tổng giám đốc.

Hành động không tuân thủ chính sách có thể dẫn đến hành động kỷ luật, tùy theo mức độ thì có mức xử lý khác nhau.

* **Tiêu chuẩn, chính sách liên quan**

ISO 27001

## Chính sách nhân sự

* **Trước khi tuyển dụng**

1. Nhân viên ứng tuyển vào công ty phải trải qua vòng phỏng vấn, cần kiểm tra những điều sau:

* Kiểm tra danh tính (giấy phép lái xe, hộ chiếu, CMND, tài khoản ngân hàng cùng tên với người phỏng vấn, …)
* Kiểm tra bằng việc tham khảo từ nhiều mối quan hệ quen biết hoặc các phương tiện truyền thông đại chúng.
* Xác nhận trình độ học vấn hoặc trình độ học vấn hoặc trình độ chuyên môn phù hợp.
* Kiểm tra hồ sơ phạm tội cho các vị trí ứng tuyển cao.

Nếu nhân viên đó đang được tuyển dụng thông qua một bên thứ 3 hoặc một công ty khác, thì công ty đó phải thực hiện kiểm tra sàng lọc phù hợp với các quy định nêu trên.

2. Thông tin cá nhân của nhân viên tiềm năng phải được đảm bảo bí mật áp dụng trên luật pháp và các quy định có liên quan. Việc truy cập này cũng cần phải được giới hạn lại, chỉ những bộ phận hoặc người có liên quan mới được biết.

3. Tất cả các nhân viên phải đồng ý tuân thủ Chính sách của công ty (đặc biệt là chính sách An toàn bảo mật thông tin) trước khi vào làm việc chính thức. Ngoài ra, nhân viên có thể được yêu cầu ký một thỏa thuận không tiết lộ vai trò của họ về quyền truy cập vào thông tin nhạy cảm.

* **Trong quá trình làm việc**

1. Nhân viên (kể cả thực tập sinh) định kỳ phải tham gia và hoàn thành khóa học nâng cao nhận thức về an toàn an ninh thông tin phù hợp và cập nhật thường xuyên các quy chế, chính sách và thủ tục liên quan đến vai trò của họ.

2. Chương trình nâng cao nhận thức an toàn an ninh thông tin phải bao gồm 2 phần:

* Nhận thức chung về an ninh thông tin.
* Chính sách, tiêu chuẩn về an ninh thông tin.

3. Việc không tuân thủ Chính sách và Tiêu chuẩn về an toàn an ninh thông tin có thể dẫn đến hành động kỷ luật, tùy theo mức độ thì có mức xử lý khác nhau.

* **Thôi việc hoặc thay đổi công việc**

1. Quản lý của nhân viên đó phải thông báo cho tất cả mọi người về việc chấm dứt của nhân viên.

2. Nhân viên từ chức/thay đổi công tác phải thông báo cho quản lý trước 1 tháng kể từ ngày chính thức thôi việc để quản lý có thể sắp xếp người bổ sung vào vị trí đó.

3. Tài khoản và quyền truy cập vào tất cả các hệ thống của công ty phải được thay đổi hoặc xóa bỏ trước 24 giờ kể từ ngày kết thúc hợp đồng.

4. Quyền truy cập của nhân viên được xem xét bất cứ khi nào vai trò của nhân viên đó bị thay đổi. Quản lý chịu trách nhiệm về việc xem xét này, tức là không xóa bỏ hoàn toàn mà chỉ disable, khi cần thiết có thể ủy quyền lại cho người khác.

5. Nhân viên nghỉ việc phải tiến hành bàn giao tài sản, bao gồm những tài sản thuộc về công ty như chìa khóa, máy tính, thẻ nhân viên, dữ liệu hoặc tài liệu có liên quan đến công ty, …

* **Tuân thủ chính sách**

Hoạt động giám sát việc tuân thủ chính sách sẽ do HR và quản lý của nhân viên đó trực tiếp giám sát.

Tất cả các yêu cầu ngoài những quy định trên sẽ phải được kiểm tra, đánh giá và được sự chấp thuận của tổng giám đốc hoặc quản lý của các bộ phận có liên quan.

Việc không tuân thủ Chính sách và Tiêu chuẩn về an toàn an ninh thông tin có thể dẫn đến hành động kỷ luật, tùy theo mức độ thì có mức xử lý khác nhau.