


Information Of The Document

AdditionalID : 0-PR-003
EICID : DOCS-PR0000000003 Version : 31
Doc. Name : Information security policy
StartEff : 05/10/2024
EndEff :
CreatedBy : 10559
CreatedDate : 05/08/2024
UnitID : SES_ISO
Section : SES
DocCategory : Doc-Internal

EFFECTIVE**List of approval step**

Approver	ApprovedDate	Status	UnitID
10455-Danh Nhu	05/09/2024 07:19:40	Approved	SES
10118-Nguyễn Bảo Trâm	05/10/2024 11:29:55	Approved	EMRQMR

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN				
0-PR-003	Version: 31	Effective date: DMS date	Page: 1	

INFORMATION SECURITY POLICY

Index/Mục Lục

1	PURPOSE / MỤC ĐÍCH:	2
2	SCOPE / PHẠM VI ÁP DỤNG:	2
3	POLICY / CHÍNH SÁCH:	2
3.1	Information / Thông tin	2
3.2	Software / Phần mềm	2
3.3	Hardware / Phần cứng	3
3.4	Antivirus system/Hệ thống ngăn ngừa sâu máy tính	3
3.5	Internet	3
3.6	Email/Thư điện tử	4
3.7	Printing control/ Quản lý in ấn	6
3.8	Common rule for using computer/Quy định chung đối với việc sử dụng máy tính của công ty	6
3.9	Rule for portable equipment/Quy định cho thiết bị di động	8
3.9.1	Procedure for control laptop/ Quy trình giám sát Laptop	8
3.9.2	Checking schedule for Laptop/Lịch kiểm tra máy tính xách tay	9
3.9.3	Control FOV's USB	10
3.9.4	Control Guest's USB	10
3.10	Computer naming convention/Quy định về cách đặt tên máy tính	10
3.11	Password /Mật khẩu	11
3.12	Network security/An toàn mạng	11
3.13	Tuân Thủ Theo Luật An Toàn Thông Tin Mạng/ Compliance Network Information Safety Law	13
3.13.1	Những Quy Định Chung/ General rules	13
3.13.2	Bảo Đảm An Toàn Thông Tin Mạng/ To Ensure Safety Network Information	13
3.13.3	Điều Khoản Thi Hành/ Enforcement Terms	14
3.14	Wireless Network Security/Mạng không dây	15
3.15	Telephone-Fax/Hệ thống điện thoại-Fax	15
3.16	Intellectual property/Sở hữu trí tuệ	15
3.17	Outsite access/Truy cập từ bên ngoài	16
3.18	Permission on High Importance Servers/Quyền truy cập các server quan trọng	17
4	ENFORCEMENT / THI HÀNH	17
5	RESPONSIBILITIES / TRÁCH NHIỆM	17
6	APPENDIX: TEST/QUIZ	18
7	REVISION HISTORY	22

Checked by: Danh Nhu Date: DMS date	Approved by: Nguyễn Bảo Trâm Date: DMS date
Prepared by: Trình Dong Nam Date: 01-Apr-2024	Original: Võ Đức Thảo Date: 19-Sep-2007

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Effective date: DMS date

Page: 2



1 PURPOSE / MỤC ĐÍCH:

- The purpose of the FOV's Security Policy is to specify requirements, policies, basic guidelines, for company in managing security information, IT transaction and intellectual property related to Data, Hardware, Software, etc.

Mục đích của chính sách bảo mật này là đưa ra các yêu cầu, quy định, hướng dẫn cơ bản, để quản lý thông tin mật, các giao dịch về IT và sở hữu trí tuệ liên quan đến dữ liệu, phần cứng và phần mềm, v.v.

2 SCOPE / PHẠM VI ÁP DỤNG:

- The scope of this policy covers all FOV's employees, consultants and vendor/third parties' assigned persons working for FOV using network computer. All electronic communication mediums as well as all storage media & physical areas of the office and/or Factory.

Phạm vi áp dụng bao gồm tất cả nhân viên của FOV, các nhà tư vấn, cung cấp dịch vụ, sản phẩm, hàng hóa, tổ chức thứ ba làm việc tại FOV có sử dụng hệ thống mạng máy tính. Tất cả các phương tiện lưu trữ, phương tiện điện tử và bao gồm các khu vực trong văn phòng, nhà máy của FOV.

3 POLICY / CHÍNH SÁCH:

3.1 Information / Thông tin

- Security information is everyone's responsibility every day. All employees of the FOV must follow the security policies and any other regulations applicable to their area.

Bảo mật thông tin là trách nhiệm hàng ngày của mỗi nhân viên. Tất cả nhân viên của FOV phải tuân thủ chính sách bảo mật này và các quy định khác áp dụng tại bộ phận mình đang làm việc.

- Prohibit to disclose company's confidential information data to outside, such as: Financial data, R&D data, customers' data, products' related-technology, and database, management System with organizational data, product design, and production methods, and all document of items listed above must have confidential signal following procedure 0-PR-001 (Control of document).

Cấm tiết lộ thông tin quan trọng ra bên ngoài như: Số liệu tài chính, số liệu nghiên cứu & phát triển, số liệu của khách hàng, công nghệ liên quan đến sản phẩm, cơ sở dữ liệu của nhà máy, dữ liệu liên quan đến hệ thống quản lý nhân sự, tài nguyên, dữ liệu thiết kế sản phẩm, phương pháp tạo ra sản phẩm. Và tất cả các tài liệu này phải có dấu hiệu bảo mật theo quy trình kiểm soát tài liệu 0-PR-001.

- It is the employee's responsibility to protect the passwords assigned. They should not share these with any other person. It is to prevent leak of information to outsiders.

Nhân viên có trách nhiệm bảo vệ mật khẩu được giao. Để ngăn ngừa rò rỉ thông tin, những mật khẩu này không được chuyển giao cho người khác khi không được phép.

- Prohibit to do improper works that are not related to company's business during working time such as playing games, surf to non-related website, exchange private e-mail, using phone for private purpose, etc.

Cấm làm các việc riêng trong giờ làm việc. Ví dụ: Chơi trò chơi, vào Internet, trao đổi email cá nhân, sử dụng điện thoại, v.v.. vào mục đích riêng trong giờ làm việc.

3.2 Software / Phần mềm

- Prohibit to store and install any illegal software on PC and Network inside FOV. The installation must be carry out by SES. With portable, trial software, SES must check license and virus before using.

Cấm lưu trữ và cài đặt các phần mềm bất hợp pháp trên máy tính, mạng máy tính thuộc FOV. Việc cài đặt chỉ được thực hiện bởi SES. Đối với những phần mềm không cần cài đặt (portable), phần mềm thử nghiệm, phải được sự kiểm tra của SES về bản quyền và virus trước khi sử dụng.

- In the case of a virus being found, the System Engineering Section (SES) should be informed immediately. The SES will investigate and take proper measures to avoid the event in future.

Trong trường hợp phát hiện có virus, phải báo ngay bộ phận Quản Lý Hệ Thống (SES). Bộ phận SES sẽ có hành động thích hợp để phòng tránh và ngăn chặn các sự cố này xảy ra trong tương lai.

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 3



3.3 Hardware / Phần cứng

- Prohibit to modify and/or connect company's hardware to the network without authorization.
Cấm thay đổi phần cứng hoặc kết nối các phần cứng này vào mạng công ty khi không được phép.
- All removable media (e.g. floppy, USB, CD, others) must be scanned for viruses before being used. These equipments must be used at Scan PC only. Some special cases need support from SES.
Trước khi sử dụng, tất cả các phương tiện lưu trữ di động phải được quét virus. Các thiết bị di động, USB chỉ được phép sử dụng tại máy Scan, trừ trường hợp đặc biệt cần có sự hỗ trợ của SES.

3.4 Antivirus system/Hệ thống ngăn ngừa sâu máy tính

- FOV uses the Antivirus software are Kaspersky and CrowdStrike Falcon antivirus to protect all computers from viruses. This product enables central management of virus protection from multiple servers. The user's computers have been protected and auto-update virus information from the server, but the network administrator must ensure that all computers have the latest antivirus definitions from the server or from the information of FJK.
- FOV sử dụng phần mềm Anti-Virus là Kaspersky và CrowdStrike Falcon để bảo vệ cho tất cả máy tính (máy tính nhân viên, máy chủ) trong nhà máy. Phần mềm này cho phép quản lý tập trung từ nhiều máy chủ khác nhau, các máy trạm được cập nhật thông tin virus tự động từ server. Trên server được lập lịch để cập nhật thông tin từ trang web của Kaspersky và CrowdStrike Falcon thường xuyên. Tuy nhiên người quản trị phải kiểm tra tình trạng cập nhật của các máy trạm thường xuyên hoặc nhận thông tin từ FJK và xử lý khi phần mềm trong máy trạm bị lỗi ảnh hưởng đến việc bảo vệ cho máy trạm đó.
- Kaspersky Anti-Virus software must be installed on all computers (including servers and workstations) connected to the FOV intranet, and "Automatic protection" feature should always be open. Devices belonging to FOV domain and able access to the internet must install CrowdStrike Falcon.
- Toàn bộ máy tính có kết nối mạng nội bộ của FOV cần được cài đặt phần mềm Antivirus (bao gồm máy chủ và máy tính nhân viên) và phải luôn mở chế độ "Tự động bảo vệ". Cài đặt phần mềm CrowdStrike Falcon đối với máy tính thuộc domain và được phép truy cập internet, các máy tính còn lại cần được cài đặt Kaspersky.
- Workstations without Anti-Virus program installed will be disconnected from the FOV network.
Các máy trạm không được cài đặt Anti-Virus phải tách rời ra khỏi mạng nội bộ của FOV.
- Network administrator has to monitor antivirus activity daily and update the antivirus definition daily. Receive information related to security from FJK which have been detected by CrowdStrike Falcon software and resolved the problems.
Quản trị mạng phải kiểm tra tình trạng của Kaspersky Anti-Virus và cập nhật thông tin virus từ trang Web của Kaspersky hàng ngày. Nhận thông tin từ FJK các vấn đề liên quan đến security được phát hiện bởi CrowdStrike Falcon và giải quyết vấn đề nếu có.
- SES configures "WSUS" function on server. Computers in the domain will be automatically updated.
SES cấu hình update tự động bằng WSUS.
- User is prohibited to stop virus-scan process by shut down the PC with any reasons.
Người sử dụng không được phép dừng trình quét virus bằng cách shutdown máy tính với bất cứ lý do nào
- User has to inform to SES about virus detection, strange problem immediately and keep the warning message in your computer.
Người sử dụng phải thông báo cho SES về bất kì trường hợp phát hiện virus hay nghi ngờ có virus để SES có hướng khắc phục.
- Schedule scan is established automatically by policy.
Lập lịch quét virus tự động từ server bằng policy.

3.5 Internet

- This is company resource.
Đây là tài sản của công ty.
- Only user who is permitted by manager/asst.manager up uses this service for their job.
Chỉ những người được phép bởi trưởng/trợ lý trưởng bộ phận mới được sử dụng dịch vụ này cho công việc.
- Reactionary, dissolute web pages are prohibited.
Những trang web phản động, khiếm nhã, đồi trụy không cho phép sử dụng.
- Any IM (Instant Message), social network and file storage services are prohibited (Tiktok, Google Talk, Skype, Facebook, Twitter, Zing, DropBox, Box...). Allow to use voice ip of Skype for calling to international. Allow using MS Teams (provided by FOV) at work.
Không được dùng tất cả các phần mềm nhắn tin qua internet, mạng xã hội và các dịch vụ lưu trữ dữ liệu (Tiktok, Google Talk, Skype, Facebook,

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 4



Twitter, Zing, Dropbox, Box...). Cho phép sử dụng chức năng gọi điện thoại của Skype để gọi điện thoại quốc tế. Cho phép sử dụng MS Teams (được cung cấp bởi FOV) trong công việc.

- SES has the right to monitor the web pages that users accessed in the Internet.

SES có quyền giám sát các hoạt động của người sử dụng internet.

- User have no permission to upload data on the Internet without approval.

User không được quyền upload dữ liệu của FOV lên Internet mà không có sự chấp thuận từ cấp quản lý.

- Avoid access, or download from untrustworthy sites or sources on the Internet.

Tránh việc truy cập, hoặc download từ những trang web hoặc nguồn không tin cậy trên Internet.

- Guests are use wireless only. This internet line is separate with FOV network. We have exception and this exception need to approve from BOM also.

Đối với khách tham quan, chỉ sử dụng internet không dây. Điểm truy cập này tách biệt với mạng nội bộ của FOV. Tuy nhiên cũng có ngoại lệ, các ngoại lệ này phải được ban giám đốc phê duyệt.

- We apply firewall system to protect FOV's network system, if user want to use a special port/protocol, user has to issue the request to SES. SES will consider for using.

FOV sử dụng tường lửa để bảo vệ hệ thống FOV với thế giới internet. Mặc định, hệ thống khóa tất cả các cổng truy cập, nếu người dùng muốn sử dụng cổng đặc biệt nào thì gửi yêu cầu đến SES. Nếu hợp lý, an toàn, SES sẽ mở cổng theo yêu cầu.

3.6 Email/Thư điện tử

- All email accounts maintained on our email systems are property of FOV. Passwords and MFA (Multi-Factor Authentication) should not be given to other people.

Tất cả hộp thư là tài sản của FOV. Người sử dụng không được phép để lộ mật khẩu và thông tin chứng thực MFA (Xác thực đa yếu tố) cho người khác.

- To ensure the proper use of FOV email system and make users aware of what FOV deems as acceptable and unacceptable use of its email system.

Phải đảm bảo tài nguyên email của công ty sử dụng đúng mục đích và hiệu quả.

- BCC should be used for difference customers, to minimize the disclosure of customer information of FOV.

Nên sử dụng hình thức BCC đối với khách hàng, để hạn chế tối đa việc lộ thông tin khách hàng của FOV.

- To protect the information, users are prohibited to send email in urgent status. User must check the receiver list, open and confirm attached file before sending.

Để đảm bảo an toàn thông tin khi sử dụng email, người sử dụng không được gấp gáp trong quá trình gửi email. Tất cả phải kiểm tra danh sách người nhận, mở và xác nhận thông tin trong file đính kèm trước khi gửi.

- It is strictly prohibited to send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an e-mail of this nature, you must promptly notify your supervisor.

Ngăn cấm gửi, chuyển những nội dung bôi nhọ, phỉ báng, công kích, phân biệt chủng tộc, khiêu dâm. Nếu bạn nhận được những thông tin này từ nhân viên trong công ty, hãy phản ánh lên cấp trên của bạn.

- Only users who are permitted by section/asst. manager up use this service for their job.

Trợ lý, trưởng bộ phận là người quy định danh sách hộp thư của bộ phận mình.

- User has to use his name to send email, not use his email address.

Người sử dụng phải sử dụng tên họ đầy đủ khi gửi email, không được sử dụng địa chỉ email thay cho tên người gửi.

- Immediately delete (don't open) all emails that the sender or subject is not recognized. Emails with attached attachments contain virus signatures, spam emails containing: .exe, .vbs, .js,...

Lập tức xóa (không được mở) những email không xác định được tên họ người gửi hay chủ đề của email. Những email, file có link lạ (thì không được click vào), email có file attach đính kèm có dấu hiệu nhiễm (cài) virus kèm theo, email spam có chứa các file: .exe, .vbs, .js, ..., hoặc thông tin với SES trước khi mở những email, file, link đính kèm này.

- Do not forward a message without acquiring permission from the sender first.

Không được chuyển nội dung email cho người khác khi không có sự đồng ý của người gửi.

- Note: This is un-controlled item, it belongs to "internet culture".

Chú ý: Không thể kiểm soát được vấn đề này, nó thuộc về văn hóa nhận thức của cộng đồng internet.

- Do not use auto-forward feature to forward email to outside email address without approval.

Không được sử dụng tính năng tự động chuyển email để chuyển email tới địa chỉ email bên ngoài FOV mà chưa được phê duyệt.

- Do not forge or attempt to forge email messages.

Không được giả mạo thông tin trong email.

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 5



- Do not send email messages using another person's email account.
Không được sử dụng tài khoản thư điện tử của người khác để gửi email.
- Do not copy a message or attachment belonging to another user without permission of the originator.
Không được sao chép thông tin hoặc file đính kèm cho người khác khi chưa được sự cho phép của người gửi.
- Do not disguise or attempt to disguise your identity when sending mail.
Không được che dấu thông tin cá nhân khi gửi email (Ví dụ: Không sử dụng tên thật khi gửi email).
- The forwarding of chain letters, junk mail, jokes and executables is strictly forbidden.
Tuyệt đối ngăn cấm việc chuyển các email rác, lừa giỡn hay các file thực thi được (.exe, *.com, *.bat...).*
- Do not use FOV's registered mailbox to do business or individual jobs.
Không được đăng ký địa chỉ email mà FOV cung cấp cho mình vào những danh mục đích kinh doanh cá nhân, không liên quan đến công việc.
- All messages distributed via the company's email system are FOV property.
Tất cả thông tin phân phối qua hệ thống của FOV là tài sản của FOV.
- Messages must include the following important notice and relate to company job.
Tất cả thông tin phải bao gồm những chú ý quan trọng, liên quan đến công việc.
- In case of guest, need the request from manager/ asst. manager up to open account, email address to use this service.
Trong trường hợp khách, chuyên gia, trợ lý, trưởng bộ phận trở lên phải ban hành yêu cầu mở hộp thư thì mới được sử dụng dịch vụ này.
- As a part of the email service, FOV provides users with 100 Gigabytes (GB) of email storage for storage emails. Users can use our mailbox management facilities and save important emails to their own computers.
Như một phần của hệ thống email, FOV cung cấp dung lượng khoảng 100 GB trên server để lưu trữ email. Người dùng có thể sử dụng tính năng quản lý hộp thư để lưu email quan trọng về máy tính.
- When using FOV email users must not send email, messages or attachments which are larger than 30MB. Email system automatically returns all email messages and attachments to users if they are larger than 30MB. In case the email recipient is a partner outside of Fujikura Group, they will receive emails with an attachment size according to the policy of their company.
Khi sử dụng email, người dùng không được gửi file đính kèm vượt quá 30Mb. Hệ thống sẽ trả lại những email có kích thước quá 30Mb. Trường hợp người nhận mail là đối tác bên ngoài tập đoàn Fujikura sẽ nhận được mail với dung lượng file đính kèm theo chính sách của công ty đối tác.
- Use zip method before send to reduce the time to send. Or request FTP service in case need to send large capacity outside.
Sử dụng giải pháp nén file trước khi gửi để giảm thời gian và tài nguyên internet của công ty. Hoặc sử dụng dịch vụ FTP để thay thế trong trường hợp cần gửi dung lượng lớn ra bên ngoài.
- SES may change this rule at any time by changing or removing existing terms or adding new ones. SES will inform users about any changes by posting an updated rule on our Intranet Web site.
SES có thể thay đổi nội dung quy định này cho phù hợp với thực tế của công ty. SES sẽ thông báo nội dung thay đổi trên trang web nội bộ của công ty.

31

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 6



3.7 Printing control/ Quản lý in ấn:

- Print only necessary documents. Prepare enough white paper before printing. In case you want to cancel the printing job, get the paper out and inform to SES for support.
Chỉ in những tài liệu cần thiết cho công việc, phải chuẩn bị đủ giấy trước khi in. Trong trường hợp muốn hủy lệnh in, lấy giấy ra khỏi máy in và thông báo ngay cho SES để được hỗ trợ.
- Keeping economical spirit to minimize the wasting of paper and ink.
Trên tinh thần tiết kiệm, đảm bảo quá trình in ấn hiệu quả, tiết kiệm giấy, mực.
- No personal printing is acceptable. If a user were found printing private stuff, admin would give warning, a fine or cutting off printing right of that user.
Không chấp nhận việc in ấn tài liệu cá nhân. Nếu vi phạm sẽ bị kỷ luật và có thể bị cấm sử dụng máy in.
- Everybody can inform SES if found someone printing private or very large document when many jobs are waiting. Based on importance or priority of the document, administrator can stop printing task or have appropriate action.
Khi cần in gấp trong lúc có quá nhiều lệnh in ưu tiên hơn. Hãy nhờ SES hỗ trợ.
- Administrator grants printing right and monitor printing jobs.
Nhân viên quản trị có nhiệm vụ cấp/xóa quyền sử dụng máy in theo yêu cầu và giám sát các lệnh in.

3.8 Common rule for using computer/Quy định chung đối với việc sử dụng máy tính của công ty.

- All computers are use for FOV business only.
Tất cả máy tính phải được sử dụng vào mục đích kinh doanh của công ty.
- Administrator password is controlled by SES.
Mật khẩu Admin do SES quản lý.
- User account is granted the “Power” right only except special case.
Người dùng chỉ được phân quyền “Power” ngoại trừ trường hợp đặc biệt.
- Users have to take full responsibility for using his computer.
Người sử dụng chịu trách nhiệm hoàn toàn về máy tính được giao sử dụng.
- Any software installation is carried out by SES.
Tất cả quá trình cài đặt phần mềm do SES phụ trách.
- USB (include camera, mobile set) equipment, CD Rom, memory stick is allowed at Scan machine only. Using USB equipment at user’s computer must be approved by manager and SES.
Thiết bị USB (thẻ nhớ, máy ảnh, thiết bị di động có giao tiếp USB), CD Rom chỉ cho phép sử dụng tại máy Scan. Sử dụng USB tại máy của người dùng phải được chấp thuận của trưởng bộ phận và SES.
- Media file (music, film), game, software resource is prohibited to store in user’s computer.
Các tập tin đa truyền thông (nhạc, phim, hình ảnh động...), trò chơi, nguồn cài đặt phần mềm không được lưu trên máy tính cá nhân.
- All computers must be labeled with an information security warning.
Tất cả máy tính phải được dán nhãn cảnh báo bảo mật thông tin.
- Prohibit to use private properties to carry out any company task with any reason. Individuals are fully responsible for their private properties.
- Exception:
 - Allow other devices to supply authentication code using Microsoft, Google and Sophos Authentication application only.
 - Allow to access webmail Microsoft 365, Microsoft Outlook, and Microsoft Teams on personal devices.
 - Allow VPN on mobile devices with Kaspersky antivirus protection. VPN on mobile devices will be applied for the management group to support urgent cases.
- Cấm sử dụng tài sản cá nhân để thực hiện bất kỳ công việc gì liên quan tới công ty với bất cứ lý do gì. Cá nhân hoàn toàn chịu trách nhiệm về tài sản cá nhân của mình.
Ngoại lệ:
 - Cho phép các thiết bị khác cung cấp mã xác thực từ các ứng dụng cấp mã của Microsoft, Google hoặc Sophos.
 - Cho phép dùng web mail của Microsoft 365, Microsoft Outlook, Microsoft Teams trên thiết bị cá nhân.
 - Cho phép dùng VPN trên thiết bị di động có cài đặt phần mềm bảo vệ (Kaspersky). VPN áp dụng cho nhóm quản lý cấp cao để giải quyết các tình huống khẩn cấp.
- All electronic data but not limited to information exchanged via email, software and electronic database are the property of the company. The

31

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 7



Company reserves the right to collect, store, control, monitor and use the work as required

Toàn bộ dữ liệu điện tử nhưng ko giới hạn bao gồm thông tin trao đổi qua email, phần mềm và cơ sở dữ liệu điện tử là tài sản của công ty. Công ty có toàn quyền thu thập, lưu trữ, kiểm soát, theo dõi và sử dụng theo yêu cầu của công việc

UNCONTROL COPY IF PRINTOUT

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

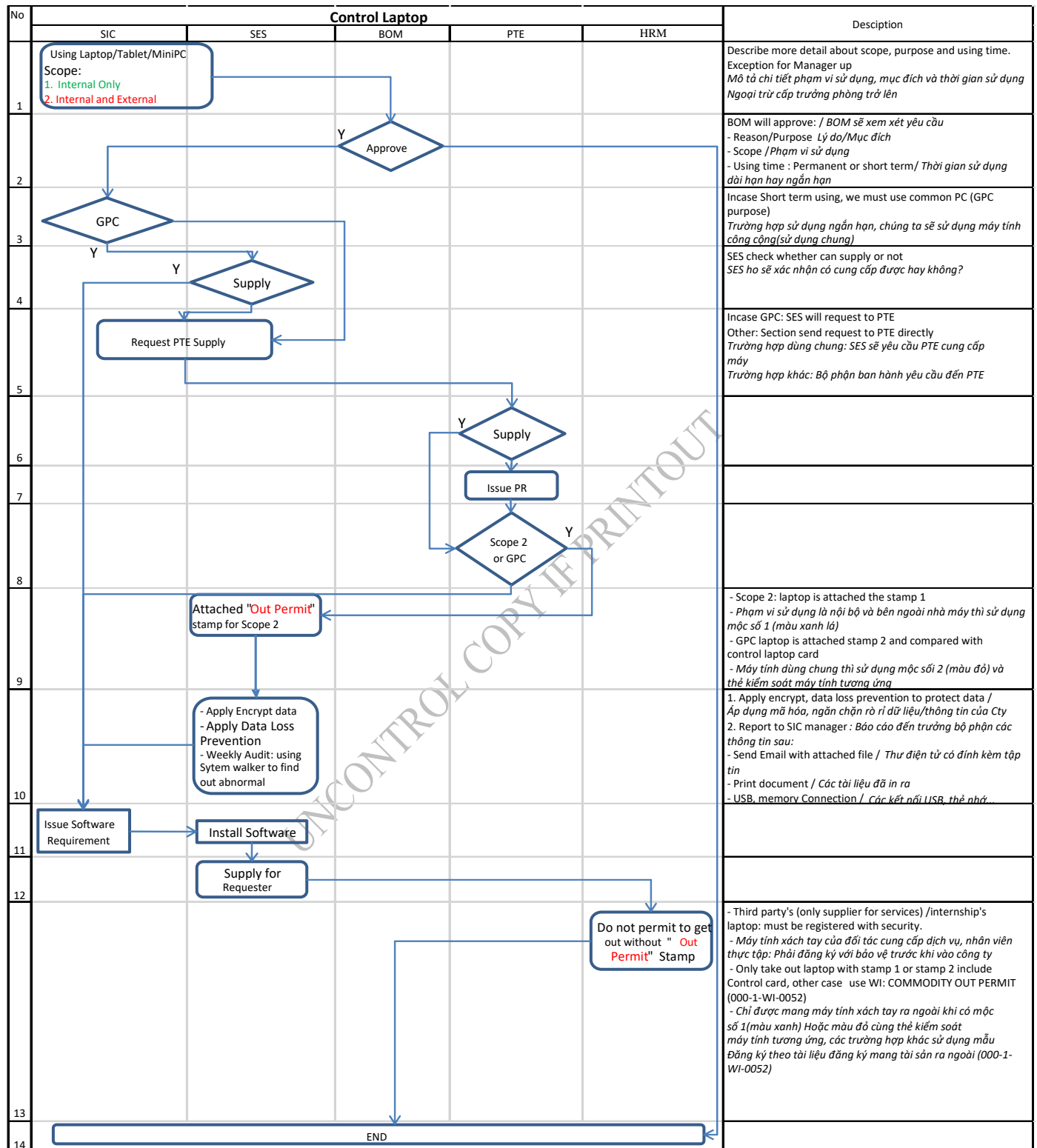
Version: 31

Page: 8



3.9 Rule for portable equipment/Quy định cho thiết bị di động

3.9.1 Procedure for control laptop/ Quy trình giám sát Laptop:



INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 9



3.9.2 Checking schedule for Laptop/Lịch kiểm tra máy tính xách tay:



Stamp 1



Stamp 2



Control laptop card compare with stamp 2

THẺ KIỂM SOÁT MÁY
TÍNH XÁCH TAYPhải trình thẻ này cho nhân viên bảo vệ
khi mang máy tính xách tay ra khỏi FOVKhi mất thẻ phải báo ngay cho
SES và HRM

CONTROL LAPTOP CARD

Must show this card when
bringing laptop out

Inform SES if this card is lost

- **External using:** Checking when follow-checking list come back.

Sử dụng bên ngoài cty: Kiểm tra khi mang máy tính xách tay mang vào cty theo danh sách kiểm tra.

- Rule for check list/ Quy định về danh sách kiểm tra:

- When laptop is scanned out → Add into check list.

Khi máy tính được quét ra → Thêm vào danh sách kiểm tra.

- Laptop in check list unless checked by SES → After SES checked → Remove out check list.

Máy tính vẫn nằm trong DS kiểm tra nếu như chưa được kiểm tra bởi SES → Sau khi SES đã kiểm tra → Xóa khỏi DS kiểm tra.

- After remove out check list, if laptop is scanned out → Add into check list again.

Sau khi xóa khỏi DS kiểm tra, nếu máy tính được quét ra → Thêm lại vào DS kiểm tra.

- Rule for checking schedule and Notification email/Quy định về lịch kiểm tra và email thông báo:

- Software will get x laptop in check list → add into checking schedule and send notification email for User (x is quantity of laptop/day need to check and defined in software by SES).

Phần mềm sẽ lấy x máy tính trong DS kiểm tra → đưa vào lịch kiểm tra và gửi email thông báo cho người dùng tương ứng (x là số lượng máy tính cần kiểm tra trong 1 ngày và được định nghĩa trong phần mềm bởi SES).

- SES will remotely check laptop follow this checking schedule.

SES sẽ kiểm tra từ xa những máy tính theo lịch kiểm tra trong ngày.

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 10

**3.9.3 Control FOV's USB:**

- Removable devices must be encrypted.
Thiết bị lưu trữ di động phải được mã hoá.
- Central control by SES.
Được quản lý bởi SES.
- Register for each using.
Phải đăng ký mỗi lần sử dụng.
- Encrypted key will be changed periodically, user must erase contents before sending back.
Mật khẩu mã hoá sẽ được thay đổi định kỳ, người dùng phải xóa dữ liệu lưu trong USB trước khi trả lại SES.

3.9.4 Control Guest's USB:

- Accept using at Scan PC only.
Chỉ được sử dụng ở máy Scan.
- SES check and grant access right for each time.
Phải được sự chấp nhận từ SES mỗi lần sử dụng.

3.10 Computer naming convention/Quy định về cách đặt tên máy tính

- IT has responsibility to set/change computer and server name.
Nhân viên quản trị có trách nhiệm đặt/thay đổi tên máy tính.
- Computer name at Office area: Account name/Tên máy tính ở khu vực văn phòng chính là tên tài khoản mạng.
 - For example: Full name Tran Thi Mai Lan, Account name: LanTTM, Computer name: LanTTM.
Ví dụ: Họ tên đầy đủ là Trần Thị Mai Lan thì tên tài khoản mạng là LanTTM và tên máy cũng là LanTTM.
- Incase of the same name: we can change/Trong trường hợp trùng tên, có thể thay đổi quy cách này.
Computer name at Leader area/Tên máy tính ở khu vực quản lý chuyên: X_YNo._Z.
 - X: Name of section/tên của bộ phận.
 - YNo.: Y is position/vị trí; No. is number/số.
 - Z: name of line/tên của chuyền.
 - EX: P2_sleader1_Maget (P2: PRD2; sleader1: Senior Leader 1; Maget: Magetsuyo).
 - Computer name at product network is machine code (xxxOPCxxxx)
Tên máy tính ở mạng sản xuất chính là số quản lý máy tính.
- Users are not permitted to change computer name.
Người sử dụng không có quyền thay đổi tên máy tính.
- Naming for Laprop: Has the _LT at the last.
Đặt tên cho Laptop sẽ có chữ _LT phía sau.

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 11



3.11 Password /Mật khẩu

Scope/Phạm vi áp dụng.

- This rule apply to all authenticated user in VLAN Office, Leader subnet.

Áp dụng để xác thực cho tất cả các user thuộc subnet văn phòng, leader.

Purpose/Mục đích

- To assure that only authenticated user can access information resource.

Để đảm bảo chỉ những người sử dụng hợp lệ mới truy cập hệ thống thông tin của công ty.

- Password must be stored in non-clear text.

Mật khẩu phải được mã hóa.

- User must change the password at the first time login on.

Người dùng phải thay đổi mật khẩu khi lần đầu tiên đăng nhập vào hệ thống.

- Password must not be shared to another with any reason.

Mật khẩu không được chia sẻ cho người khác với bất cứ lý do nào.

- If the password is in doubt, it must be changed immediately. Contact Help Desk to support if need.

Nếu mật khẩu bị rò rỉ, phải thay đổi ngay. Hoặc liên hệ nhân viên SES để được hỗ trợ.

- User is prohibited to get another user's password with any means.

Người sử dụng không được "ăn cắp" mật khẩu của người khác bằng bất cứ phương tiện nào.

- Enable "Password Protected Screensaver" after 5 minutes. Lock the PC when leave out.

Bật chế độ "Màn hình chờ" sau 5 phút, yêu cầu nhập mật khẩu khi thoát khỏi chế độ này. Khi rời khỏi vị trí, phải khóa máy tính lại.

- Guest Account should be assigned the expired date.

Tài khoản Guest phải được gán ngày hết hạn.

- User and Administrator account should be locked after 5 times un-success login on.

Tài khoản của user và quản trị sẽ bị khóa sau 5 lần đánh sai mật khẩu.

- Minimum Password length is 8 characters, for Administrator is 9 characters.

Chiều dài tối thiểu đối của mật khẩu đối với user là 8 ký tự, đối với tài khoản quản trị là 9 ký tự.

- Account lockout duration in 5 minutes for user and 30 minutes for Administrator.

Thời gian tài khoản tự động unlock là 5 phút đối với user, 30 phút đối với tài khoản quản trị.

- Minimum Password age is 0 day for users, for Administrator is 1 day.

Thời gian thay đổi password tối thiểu cho user là 0 ngày, đối với tài khoản quản trị là 1 ngày.

- Password history for user and Administrator are 3 time.

Số lần để lưu history của password là 3 lần đối với user và tài khoản quản trị.

- Password must not be user name, user birthday, easy identified word: "password", "my love"..., famous movie/place: "titanic", "hollywood" ...

Mật khẩu không được là tên tài khoản, ngày sinh nhật của người sử dụng hay những từ dễ nhận dạng như "password", "mylove" hay những cụm từ nổi tiếng như "titanic", "hollywood".

- Password must be complex.

Mật khẩu phải phức tạp.

- Password for user must be changed after 90 calendar days. Administrator password must be changed every 60 calendar days.

Mật khẩu cho user phải được thay đổi sau 90 ngày. Mật khẩu quản trị phải thay đổi sau 60 ngày.

- User has to know the current password before changing to assure you are authenticated user.

Người sử dụng phải biết mật khẩu của mình trước khi thay đổi để đảm bảo bạn là người chủ sở hữu thật sự.

- VPN user need to use complex password to reduce the risk of violation.

Những người sử dụng VPN phải áp dụng cách đặt mật khẩu tích hợp để hạn chế rủi ro.

- Help Desk will instruct user change password when the device is delivered.

Nhân viên SES sẽ hỗ trợ bạn thay đổi mật khẩu.

3.12 Network security/An toàn mạng

Scope/Phạm vi áp dụng:

- All communication (internal, external) using PC system will be treated by this rule.

Tất cả kênh thông tin (bên trong, bên ngoài) có sử dụng máy tính đều bị kiểm soát bởi quy định này.

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 12



- Firewall is required between external and internal network, between different segments also.
Tường lửa bảo vệ là yêu cầu bắt buộc giữa thế giới bên ngoài và mạng nội bộ, giữa các mạng nhỏ với nhau.
- Network infrastructure is designed by SES only and need approve from BOM.
Hạ tầng mạng được thiết kế bởi SES và phải được chấp nhận bởi ban giám đốc.
- SES must approve all network equipments (router, modem, switch, hub, access point, client PC) connect to Fov's network.
Tất cả các thiết bị mạng kết nối với mạng nội bộ phải được đồng ý bởi SES.
- DNS, DHCP, VPN, Static IP must be configured by SES only.
DNS, DHCP, VPN, IP tĩnh... chỉ được cấu hình bởi nhân viên SES.
- To prevent unauthenticated connection, all service (hosting, join domain, file and printer sharing, establish connection...) must be done by SES.
Để ngăn chặn các kết nối không hợp lệ, tất cả các dịch vụ, kết nối... phải do SES thực hiện.
- The number of VPN users is limited, only assigned account by manager up can use. Password authentication must be applied and user must applied complex password. Security audit must be setup and review log file weekly.
Số lượng người dùng VPN là giới hạn, do đó chỉ những người được cho phép bởi trưởng bộ phận trở lên mới được sử dụng. Các yêu cầu về mật khẩu phải được áp dụng. Các đánh dấu quá trình truy cập phải được ghi nhận và xem xét hàng tuần.
- SES is responsible to keep all network device up to date.
SES có nhiệm vụ cập nhật trình điều khiển, bảo mật cho tất cả thiết bị mạng.
- Login on the system with non-assigned account is prohibited.
Ngăn cấm đăng nhập vào mạng bằng những tài khoản không hợp lệ.
- Inform to SES any doubt that maybe effect to your job/data.
Thông báo cho SES biết bất kì nguy cơ có thể ảnh hưởng đến công việc hay dữ liệu của bạn.
- Fov's members are Responsible to prevent and denounce un-authorization actions.
Tất cả thành viên FOV có trách nhiệm bảo vệ và ngăn chặn hành động không hợp lệ.

UNCONTROL COPY IF PRINTOUT

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 13



3.13 Tuân Thủ Theo Luật An Toàn Thông Tin Mạng/ Compliance Network Information Safety Law

- Quote from the provisions of Law No. 86-2015-QH13 relating to the rights and obligations of organizations / individuals to comply (Reference with No. 86-2015-QH13).

Trích những quy định của luật số 86-2015-QH13 liên quan tới quyền và nghĩa vụ của tổ chức/cá nhân phải tuân thủ (tham khảo toàn bộ nội dung ở luật số 86-2015-QH13).

3.13.1. Những Quy Định Chung/ General rules:

- **Điều 4.** Principles to ensure network information safety/ Nguyên tắc bảo đảm an toàn thông tin mạng:
- Organizations and individuals must not infringe safety network information of organizations and other personal.
Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.
- **Điều 7.** Các hành vi bị nghiêm cấm/ Behavior prohibited.
 - *Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật*
Preventing the transmission of information on the network, intercedes, access, harm, delete, change, copy and falsifying information on the network is unlawful.
 - *Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng*
Influence, unlawful to the normal operation of information systems, or to the possibility to access the information system of the user.
 - *Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.*
Attack, disable unlawful and neutralize the safety method to protect the safety information of information systems; attacks, hijacking, destroy information systems.
 - *Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.*
Spread the spam email, malware, establish information systems fake, cheat.
 - *Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.*
Collect, use, distribute, illegal trading of personal information of others; taking advantage of loopholes and weaknesses of information systems to collect, exploit personal information.
 - *Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.*
Unlawful intrusion confidential information encrypted and encrypted by legitimate agencies, organizations and individuals; disclose information about civil cryptography products, customer information using cryptographic legitimate civilian products; use and trading of civil cryptography products of unknown origin.

3.13.2. Bảo Đảm An Toàn Thông Tin Mạng/ To Ensure Safety Network Information.

- **Mục 1.** Bảo Vệ Thông Tin Mạng/ Protecting Network Information.
 - **Điều 10.** Quản lý gửi thông tin/ Management of sending information.
 - *Việc gửi thông tin trên mạng phải bảo đảm các yêu cầu sau đây:*
- The information sent over the network must ensure the following requirements:
 - Không giả mạo nguồn gốc gửi thông tin;*
 - Don't fake the origin sending information;
Tuân thủ quy định của Luật này và quy định khác của pháp luật có liên quan.
 - Keep rule of this Law and other provisions of relevant laws.
Tổ chức, cá nhân không được gửi thông tin mang tính thương mại vào địa chỉ điện tử của người tiếp nhận khi chưa được người

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 14



tiếp nhận đồng ý hoặc khi người tiếp nhận đã từ chối, trừ trường hợp người tiếp nhận có nghĩa vụ phải tiếp nhận thông tin theo quy định của pháp luật.

- Organizations and individuals are not allowed to send commercial information to the electronic address of the recipient if the recipient has not been agreed or refused, except in cases where the recipient is obliged to receiving information in accordance with the law.
- **Điều 11.** Phòng ngừa, phát hiện, ngăn chặn và xử lý phần mềm độc hại/ Preventing, detecting, and dealing with malware.
- Cơ quan, tổ chức, cá nhân có trách nhiệm thực hiện phòng ngừa, ngăn chặn phần mềm độc hại theo hướng dẫn, yêu cầu của cơ quan nhà nước có thẩm quyền.
- Agencies, organizations and individuals are responsible for implementation of prevention, preventing malicious software under the guidance and requirements of government agencies having jurisdiction.
- **Điều 15.** Trách nhiệm của cơ quan, tổ chức, cá nhân trong bảo đảm an toàn thông tin mạng/ The responsibilities of agencies, organizations and individuals in ensuring the safety information network.
Cơ quan, tổ chức, cá nhân sử dụng dịch vụ trên mạng có trách nhiệm thông báo kịp thời cho doanh nghiệp cung cấp dịch vụ hoặc bộ phận chuyên trách ứng cứu sự cố khi phát hiện các hành vi phá hoại hoặc sự cố an toàn thông tin mạng.
- Agencies, organizations and individuals using network services have a duty to announce to the enterprise provide service or specialized department to rescue on time when detect actions of vandalism or trouble about safety network information.
- **Mục 2.** Bảo Vệ Thông Tin Cá Nhân/ **Protecting Personal Information**
Điều 16. Nguyên tắc bảo vệ thông tin cá nhân trên mạng/ Principle of protection of personal information on the network.
Cá nhân tự bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng.
- Individuals protect their personal information and comply with the provisions of the law on providing personal information when using network services.
Điều 18. Cập nhật, sửa đổi và hủy bỏ thông tin cá nhân/ Update, modify and cancel the personal information.
Chủ thể thông tin cá nhân có quyền yêu cầu tổ chức, cá nhân xử lý thông tin cá nhân cập nhật, sửa đổi, hủy bỏ thông tin cá nhân của mình mà tổ chức, cá nhân đó đã thu thập, lưu trữ hoặc ngừng cung cấp thông tin cá nhân của mình cho bên thứ ba.
- Personal of information has the right to request the organizations and individuals that handle personal information to update, modify, cancel their personal information by organizations individuals that collect, store, or stop provide your personal information to third parties.
- **Mục 4.** Ngăn Chặn Thông Tin Xung Đột Trên Mạng/ **Prevention Conflict Information on Network.**
Điều 28. Trách nhiệm của tổ chức, cá nhân trong việc ngăn chặn xung đột thông tin trên mạng/ Responsibilities of organizations and individuals in conflict prevention information online.
Tổ chức, cá nhân trong phạm vi nhiệm vụ, quyền hạn của mình có trách nhiệm sau đây:
- Organizations and individuals within the duties and powers, be responsible for the following:
Ngăn chặn thông tin phá hoại xuất phát từ hệ thống thông tin của mình; hợp tác xác định nguồn, đẩy lùi, khắc phục hậu quả tấn công mạng được thực hiện thông qua hệ thống thông tin của tổ chức, cá nhân trong nước và nước ngoài;
- Prevent destructive information derived from information systems; determine resource, repel, resolve the results of network attacks that through the information system of organizations and individuals at home and abroad;
Ngăn chặn hành động của tổ chức, cá nhân trong nước và nước ngoài có mục đích phá hoại tính nguyên vẹn của mạng;
- Prevent actions of organizations and individuals at home and abroad with the purpose of undermining the integrity of the network;
Loại trừ việc tổ chức thực hiện hoạt động trái pháp luật trên mạng có ảnh hưởng nghiêm trọng đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội của tổ chức, cá nhân trong nước và nước ngoài.
- Excluding the organization of illegal activity on the Internet has seriously affected the defense, national security and order, social security organizations and individuals at home and abroad.

3.13.3. Điều Khoản Thi Hành/ Enforcement Terms

- **Điều 53.** Hiệu lực thi hành/ **Enforcement Effect.**
- Luật này có hiệu lực thi hành từ ngày 01 tháng 7 năm 2016.
- This law will be affected from July 1, 2016.

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 15



3.14 Wireless Network Security/Mạng không dây

- All policies that apply for wire network will be applied for wireless network also. But we have to consider some extra requirement.
Tất cả những chính sách áp dụng cho mạng dây thì cũng sẽ áp dụng cho mạng không dây. Nhưng chúng ta sẽ xem xét thêm một số yêu cầu chuyên biệt.
- The desired coverage area must be considered and approved.
Phạm vi phủ sóng của mạng không dây phải được xem xét phù hợp, được phê duyệt trước khi tiến hành lắp đặt.
 - Design a wifi system that can meet the required number of users.
Thiết kế hệ thống wifi có thể đáp ứng đủ lượng người dùng theo yêu cầu
 - Need to monitoring of traffic usage in the wifi system to meet with using demand
Cần theo dõi lưu lượng sử dụng trong hệ thống wifi để đáp ứng nhu cầu sử dụng wifi.
- These information help us to choose compatible wireless equipment to limit un-authenticated connection.
Những thông tin này giúp quá trình chọn lựa thiết bị phù hợp với yêu cầu. Tránh được những kết nối không mong muốn.
- All Wireless equipment must be used the same 802.1x standard.
Tất cả thiết bị mạng không dây phải tương thích với chuẩn IEEE 802.1x.
- All equipment should support open authentication method: EAP (Extensible Authentication Protocol) standard.
Tất cả thiết bị phải hỗ trợ các phương pháp xác thực mật khẩu EAP.
- Password authentication is required.
Mật khẩu truy cập là yêu cầu bắt buộc.
- All wireless access point must be put in secure area.
Tất cả các thiết bị phát sóng phải đặt ở nơi an toàn.

3.15 Telephone-Fax/Hệ thống điện thoại-Fax

- This resource is used for business only.
Nguồn tài nguyên này chỉ dùng vào mục đích kinh doanh.
- Only member who was permitted by BOM can call over sea.
Chỉ những người được ban giám đốc đồng ý mới được gọi điện thoại quốc tế.
- Engineer, staff, main-gate can call to Ho Chi Minh city and mobile network for their job as default.
Kỹ sư, nhân viên văn phòng, cổng chính nhà máy mặc định được gọi về TPHCM hoặc di động phục vụ công việc của họ.
- Beside HCMC and Binh Duong province, only member who was permitted by assistant/manager up can call to another area in Viet Nam for their job.
Ngoài TPHCM và Bình Dương, chỉ những nhân viên được phép của trợ lý/trưởng bộ phận trở lên được gọi liên tỉnh cho nhu cầu công việc.
- Telephone in production line, Canteen, Driver room and Sub-Gate can call internal only.
Điện thoại trong khu vực sản xuất, canteen, phòng tài xế và các cổng phụ nhà máy chỉ được gọi nội bộ.
- The Value-added service is prohibited except for company job.
Các dịch vụ giá trị gia tăng không được sử dụng ngoại trừ công việc yêu cầu.
- The saving channel can be use for cost down (One Contact, Call thought 171,177...).
- Before Fax, please check the telephone, content and total number carefully to secure the information.
Các dịch vụ tiết kiệm được chỉ phí được khuyến dùng (One Contact, Dịch vụ 177,171...).
- Before Fax, please check the telephone, content and total number carefully to secure the information.
Trước khi Fax, phải kiểm tra thật kỹ số điện thoại, nội dung và tổng số tờ để tránh lãng phí và bảo mật thông tin.
- SES will choose the control method to assure that the resource is used efficiently.
SES sẽ chọn cách kiểm soát để đảm bảo nguồn tài nguyên này được sử dụng hiệu quả.

3.16 Intellectual property/Sở hữu trí tuệ

Definition / Định nghĩa:

- Customer property: spec, drawing, instruction...
Tài sản khách hàng: Đặc điểm cấu tạo của sản phẩm, bản vẽ, hướng dẫn...
- FOV documentation (including training material)

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 16



Tài liệu của FOV (kể cả tài liệu đào tạo).

- FOV software

Phần mềm của FOV.

- FOV drawing

Bản vẽ của FOV.

- Product

Sản phẩm.

- Equipment

Thiết bị.

- Material

Vật tư.

Policy / Chính sách.

- Intellectual property must be control strictly by FOV's member:

Sở hữu trí tuệ phải được quản lý bởi nhân viên của FOV một cách triệt để.

- Disclosure to outside FOV (by any way, method) without NDA is prohibited.

Cấm tiết lộ ra khỏi FOV (bằng bất cứ cách nào, phương pháp nào) mà không có cam kết bảo mật.

- Non-Disclosure Agreement (NDA) must be signed between both management sites before transfer Intellectual Property.

Cam kết bảo mật phải được đồng ý bằng văn bản giữa các bên liên quan trước khi chuyển giao tài sản.

- Violation: will be treat as highest level in company rule.

Vi phạm: sẽ bị xử lý ở mức cao nhất trong quy định của công ty.

3.17 Outsider access/Truy cập từ bên ngoài.

- All connections (VPN, VNC, Remote Desktop, Team viewer,...) which access from outside to FOV network system must be through firewall and approved by manager up.

Tất cả các kết nối (VPN, VNC, Remote Desktop, Team viewer,...) truy cập từ bên ngoài vào hệ thống mạng của FOV đều phải thông qua tường lửa và phải được duyệt bởi cấp trưởng bộ phận trở lên.

- VPN service is provided for employees who usually work outside. The service is also available for special require from Head Office. SES will setup and guide user to use the service.

- Dịch vụ VPN được cấp cho các nhân viên, những người thường xuyên công tác bên ngoài nhà máy. Dịch vụ này cũng phục vụ cho những yêu cầu đặc biệt từ công ty mẹ. Nhân viên SES sẽ cài đặt và hướng dẫn sử dụng dịch vụ này.

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 17



3.18 Permission on High Importance Servers/Quyền truy cập các server quan trọng.

No	Server Name	Importance security Level	Permission								
			Access into server, remote desktop	Database access	Admin for maintain, backup, turn on/off, ...	Install / Uninstall any software/firmware	Plug in/out USB or Portable HDD	Access Internet for online backup, maintain, remote support, update, down/up load	Full internet	Transfer data for backup, maintain	Transfer data (Request by email, remind... and must be approved by Manager)
1	FOVSEVR7	High	Mng, Sysadmin	Software Sysadmin (Support)	Sysadmin, Tech (support)	Need to approve	Need to approve	Sysadmin	NO	Sysadmin	Need to approve
2	FOVSEVR3	High	Mng, Sysadmin	Software Sysadmin (Support)	Sysadmin, Tech (support)	Need to approve	Need to approve	Sysadmin	NO	Sysadmin	Need to approve
3	VMWSEVR3	High	Mng, Sysadmin	Software Sysadmin (Support)	Sysadmin, Tech (support)	Need to approve	Need to approve	Sysadmin	NO	Sysadmin	Need to approve
4	FOVERP	High	Mng, Sysadmin, supporter	N/A	Sysadmin, Tech (support)	Need to approve	Need to approve	Sysadmin	NO	Sysadmin	Need to approve
5	FOVSEVR11	High	Mng, Sysadmin, supporter	N/A	Sysadmin, Tech (support)	Need to approve	Need to approve	Sysadmin	NO	Sysadmin	Need to approve
6	FovOrcBK	High	Mng, Sysadmin, supporter	Software Sysadmin (Support)	Sysadmin, Tech (support)	Need to approve	Need to approve	Sysadmin	NO	Sysadmin	Need to approve
7	Fovsevr1,2, FOVDC1	High	Sysadmin	N/A	Sysadmin, Tech (support)	Need to approve	Need to approve	Sysadmin	NO	Sysadmin	Need to approve
8	Fovdata, Fovweb	Average	Sysadmin, Software	N/A	SES	Need to approve	Need to approve	Sysadmin	NO	Sysadmin	Need to approve
9	Fovsevr6	Low	SES	N/A	Sysadmin, Tech (support)	Need to approve	Need to approve	Sysadmin	NO	Sysadmin	Need to approve
10	Others	Low	SES	N/A	Sysadmin, Tech (support)	Need to approve	Need to approve	Sysadmin	NO	Sysadmin	Need to approve

4 ENFORCEMENT / THI HÀNH

- User need to issue the request to SES for opening the legal service (Use form 000-0-Fo-001).
Người dùng phải ban hành yêu cầu sử dụng dịch vụ tới SES (Sử dụng mẫu 000-0-Fo-001).
- In the case of a violation of the security policy, disciplinary action will be taken, up to and including employment termination.
Trong trường hợp vi phạm chính sách bảo mật này, nhân viên vi phạm sẽ bị thi hành kỷ luật và có thể dẫn đến sa thải.

5 RESPONSIBILITIES / TRÁCH NHIỆM

- All employees.
Tất cả nhân viên FOV.



6 APPENDIX: TEST/QUIZ

Câu 1:

Đối với mục đích của 0-PR-003, câu trả lời nào ĐÚNG?

- ☐ Mục đích của chính sách bảo mật này là đưa ra các yêu cầu, quy định, hướng dẫn cơ bản để quản lý thông tin, các giao dịch về IT và sở hữu trí tuệ liên quan đến phần cứng và phần mềm...vv
- ☐ Mục đích của chính sách bảo mật này là đưa ra các yêu cầu, quy định, hướng dẫn cơ bản để quản lý thông tin, các dịch vụ về IT.

Câu 2:

Đối với phạm vi áp dụng, câu trả lời nào ĐÚNG?

- ☐ Phạm vi áp dụng bao gồm tất cả nhân viên của FOV có sử dụng máy tính, các nhà tư vấn, cung cấp dịch vụ, sản phẩm, hàng hóa, tổ chức thứ ba làm việc tại FOV có sử dụng hệ thống mạng máy tính. Tất cả các phương tiện lưu trữ, phương tiện điện tử và bao gồm các khu vực trong văn phòng, nhà máy của FOV.
- ☐ Phạm vi áp dụng bao gồm tất cả nhân viên của FOV, các nhà tư vấn, cung cấp dịch vụ, sản phẩm, hàng hóa, tổ chức thứ ba làm việc tại FOV có sử dụng hệ thống mạng máy tính. Tất cả các phương tiện lưu trữ, phương tiện điện tử và bao gồm các khu vực trong văn phòng, nhà máy của FOV.
- ☐ Phạm vi áp dụng bao gồm tất cả nhân viên của FOV có sử dụng máy tính. Tất cả các phương tiện lưu trữ, phương tiện điện tử và bao gồm các khu vực trong văn phòng, nhà máy của FOV

Câu 3:

Bảo mật thông tin là trách nhiệm của ai?

- ☐ Của bộ phận SES.
- ☐ Của ban lãnh đạo FOV.
- ☐ Của toàn thể cán bộ công nhân viên FOV.

Câu 4:

Những thông tin quan trọng nào cần tiết lộ ra bên ngoài?

- ☐ Số liệu tài chính.
- ☐ Số liệu nghiên cứu & phát triển.
- ☐ Số liệu của khách hàng.
- ☐ Công nghệ liên quan đến sản phẩm.
- ☐ Cơ sở dữ liệu của nhà máy.
- ☐ Dữ liệu liên quan đến hệ thống, quản lý nhân sự.
- ☐ Tài nguyên, dữ liệu thiết kế sản phẩm.
- ☐ Phương pháp tạo ra sản phẩm.
- ☐ Tài liệu có dấu hiệu bảo mật theo quy trình kiểm soát tài liệu 0-PR-001.
- ☐ Tất cả các loại tài liệu bên trên.

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 19

**Câu 5:**

Người dùng có được phép tự cài đặt phần mềm vào máy tính hay không?

- ☐ Được phép cài mà không cần thông báo.
- ☐ Có thể tự cài nếu máy tính đó có quyền Admin.
- ☐ Chỉ được cài những phần mềm miễn phí, sử dụng phần mềm portable (phần mềm không cần cài đặt).
- ☐ Không được phép, những phần mềm cần cài đặt phục vụ cho mục đích công việc phải được trưởng/ phó trưởng bộ phận đó và SES duyệt thì mới được phép cài đặt và việc cài đặt được thực hiện bởi nhân viên bộ phận SES.

Câu 6:

Đối với việc user sử dụng máy tính và hệ thống mạng: Hành động nào ĐÚNG? (Chọn nhiều đáp án)

- ☐ Chịu trách nhiệm hoàn toàn về máy tính công ty giao sử dụng.
- ☐ Tự cài đặt phần mềm, thay thế phần cứng.
- ☐ Mang thiết bị của cá nhân (máy tính xách tay) vào cty và kết nối vào hệ thống mạng của cty.
- ☐ Sao chép dữ liệu bằng cách sử dụng USB cắm vào máy tính cty.
- ☐ Cắm điện thoại vào máy tính để sạc pin hoặc sao chép dữ liệu, hình ảnh, ...
- ☐ Sao chép dữ liệu bằng cách sử dụng USB cắm vào máy tính công cộng (máy tính Scan).
- ☐ Yêu cầu SES cài đặt phần mềm, thay thế thiết bị phần cứng khi có hư hỏng.

Câu 7:

Bạn cần làm gì khi phần mềm diệt Virus (Kaspersky) thông báo máy tính bị nhiễm Virus?

- ☐ Bỏ qua và tắt thông báo.
- ☐ Người sử dụng phải thông báo cho SES về bất kỳ trường hợp phát hiện có virus hay nghi ngờ có virus.
- ☐ Restart hoặc tắt máy tính.

Câu 8:

Bạn không được phép truy cập, sử dụng các ứng dụng, dịch vụ nào trên mạng Internet? (Chọn nhiều đáp án)

- ☐ Sử dụng Skype để gọi điện liên hệ khách hàng (có sự đồng ý của cấp trên).
- ☐ Sử dụng mạng xã hội, Chat khi làm việc: Facebook, Twitter, Skype, ...
- ☐ Sử dụng dịch vụ lưu trữ trên Internet: OneDrive, Google Drive, Drop Box, ...
- ☐ Sử dụng dịch vụ lưu trữ trên Internet do công ty hoặc khách hàng cung cấp.
- ☐ Truy cập vào các trang web thuộc thể loại: Games, xem phim, nghe nhạc, phim ảnh đồi trụy

Câu 9:

Khi làm việc với Email, hành động nào ĐÚNG? (Chọn nhiều đáp án)

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 20



- ☐ Kiểm tra danh sách người nhận, mở và xác nhận thông tin trong file đính kèm trước khi gửi.
- ☐ Không gửi file đính kèm có dung lượng lớn cho group mail (chỉ gửi link của file đặt trên FileServer) và giới hạn dung lượng email được gửi < 30Mb
- ☐ Gửi email với nội dung: Giả mạo, lừa dối, bôi nhọ, phỉ báng, công kích, phân biệt chủng tộc, khiêu dâm, ...
- ☐ Lập tức xoá (không được mở) những email không xác định được tên họ người gửi hay chủ đề của email.
- ☐ Không được chuyển nội dung email, file đính kèm cho người khác khi không có sự đồng ý của người gửi.
- ☐ Được sử dụng tính năng tự động chuyển email để chuyển email tới địa chỉ email bên ngoài FOV mà không cần phê duyệt
- ☐ Sử dụng địa chỉ email của cty để sử dụng mục đích cá nhân, đăng ký vào những dịch vụ công cộng (không liên quan tới công việc) trên Internet.
- ☐ Sử dụng giải pháp nén file attach trước khi gửi đi.

Câu 10:

Trường hợp nào được phép mang Laptop ra ngoài công ty?

- ☐ Tất cả nhân viên có Laptop có thể mang ra ngoài mà không cần khai báo.
- ☐ Tất cả nhân viên có Laptop mang ra ngoài phải khai báo với SES để được đăng ký trên hệ thống, dán số quản lý thiết bị và nhãn "Out permit"
- ☐ Chỉ từ cấp quản lý (Manager) trở lên mới được mang Laptop ra ngoài.

Câu 11:

Đối với mật khẩu, hành động nào SAI? (Chọn nhiều đáp án)

- ☐ Chia sẻ mật khẩu cho người khác.
- ☐ Biết và dùng mật khẩu của người khác.
- ☐ Đặt mật khẩu với chiều dài lớn hơn 8 ký tự, admin là 9 ký tự
- ☐ Người dùng phải đổi mật khẩu sau 90 ngày, admin là 60 ngày

Câu 12:

IP tĩnh được cấu hình bởi ai?

- ☐ Bất cứ ai có quyền Admin.
- ☐ Khách hàng.
- ☐ Chuyên gia.
- ☐ SES.

Câu 13:

Đối với sở hữu trí tuệ, chọn câu trả lời ĐÚNG (Chọn nhiều đáp án)

- ☐ Cấm tiết lộ ra khỏi FOV (bằng bất cứ cách nào, phương pháp nào) mà không có cam kết bảo mật NDA.

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Page: 21



- ☐ Có thể tiết lộ ra khỏi FOV mặc dù có cam kết bảo mật NDA.
- ☐ Cam kết bảo mật phải được đồng ý bằng email giữa các bên liên quan trước khi chuyển giao tài sản.
- ☐ Cam kết bảo mật phải được đồng ý bằng văn bản giữa các bên liên quan trước khi chuyển giao tài sản.

Câu 14:

Về việc sử dụng USB, việc nào sau đây là SAI (Chọn nhiều đáp án)

- ☐ USB phải được mã hóa.
- ☐ Người dùng phải xóa dữ liệu trong USB trước khi trả lại cho SES.
- ☐ Có thể sử dụng USB trong công ty mà không cần làm thủ tục gì, miễn phục vụ cho công việc.
- ☐ Chỉ được sử dụng USB ở máy SCAN. Trừ trường hợp có approve từ cấp quản lý.

Câu 15:

Sử dụng WIFI FOVGUEST trong trường hợp nào?

- ☐ Chỉ BOM và Guest được phép sử dụng
- ☐ Chỉ cần có password thì có thể sử dụng được

Đối tượng thực hành bài test:

Đối tượng	Phạm vi làm bài	Ghi chú
All	Câu: All	Những user sử dụng máy tính (Trừ OP)

INFORMATION SECURITY POLICY/ CHÍNH SÁCH BẢO MẬT THÔNG TIN

0-PR-003

Version: 31

Effective date: DMS date

Page: 22



7 REVISION HISTORY

Preparing date	Person	Version	Description		Reason	Requester
			Old content	New content		
1-Apr-24	Trinh Dong Nam	31	3.4 Antivirus system/Hệ thống ngăn ngừa sâu máy tính 3.6 Email/Thư điện tử 3.8 Common rule for using computer/Quy định chung đối với việc sử dụng máy tính của công ty.	3.4 Antivirus system/Hệ thống ngăn ngừa sâu máy tính: Apply new antivirus Falcon application. 3.6 Email/Thư điện tử: FOV provides users with 100 Gigabytes (GB) of email storage. 3.8 Common rule for using computer/Quy định chung đối với việc sử dụng máy tính của công ty: Allow to use Microsoft 365 features email, Teams on personal devices; Allow to use VPN on mobile which has been installed antivirus application.	Review, update the document	Div.MNG Dang Cong Son
12-May-22	Nguyễn Hữu Hải Đăng	30	3.4 Antivirus system/ Hệ thống ngăn ngừa sâu máy tính 3.5 Internet 3.8 Common rule for using computer/ Quy định chung đối với việc sử dụng máy tính của công ty	3.4 Antivirus system/ Hệ thống ngăn ngừa sâu máy tính: make clear meaning 3.5 Internet: add MS Teams 3.8 Common rule for using computer/ Quy định chung đối với việc sử dụng máy tính của công ty: Allow other devices to supply authentication code using Microsoft, Google and Sophos Authentication application only	Review, cập nhật lại tài liệu	Đăng Công Sơn
29-Nov-21	Nguyễn Hữu Hải Đăng	29	3.6 Email/Thư điện tử 3.9 Rule for portable equipment / Quy định cho thiết bị di động 3.17 Outsite access/Truy cập từ bên ngoài. 3.18 Permission on High Importance Servers/ Quyền truy cập các server quan trọng APPENDIX:TEST/QUIZ	3.6 Email/Thư điện tử (Quota 30MB) 3.9 Rule for portable equipment / Quy định cho thiết bị di động Remove: Rule for Black list/Quy định về DS cấm 3.17 Outsite access/Truy cập từ bên ngoài. 3.18 Permission on High Importance Servers/Quyền truy cập các server quan trọng: Remove Fovex16 APPENDIX: TEST/QUIZ - Update Q9,Q10 - Delete Q14	Review, cập nhật lại tài liệu.	Nguyễn Hữu Hải Đăng
10-Jul-20	Nguyen Huu Duc	28	3.3 Hardware / Phần cứng	3.3 Hardware / Phần cứng	Revise làm rõ 1 số quy định (Có note màu vàng và version)	Nguyen Huu Hai Dang
17-Jan-19	Nguyen Huu Duc	27	3.9.1 Procedure for control laptop/ Quy trình giám sát Laptop	3.9.1 Procedure for control laptop/ Quy trình giám sát Laptop	Bổ sung thêm quy định cho phần thiết bị Mini PC, Tablet trong phần quy trình	Nguyen Truong Giang