MASAN GROUP	**CHÍNH SÁCH AN NINH THÔNG TIN** ***INFORMATON SECURITY POLICY***	*Mã số (Code):* MSN/IT-CSATTT-001
		Ngày ban hành (Issue date): 01/07/2024
		Ngày hiệu lực (Effective date): 01/07/2024
		Lần ban hành (Version): 1

Biên soạn *Prepared by*	**Kiểm tra** *Reviewed by*	**Kiểm tra** *Reviewed by*	**Phê duyệt** *Approved by*
Mai Trung Dũng	**Rahul Bhandari**	**Trần Phương Bắc**	**Danny Le**
Giám đốc An Toàn Thông Tin	Giám đốc Công Nghệ	Luật Sư Trưởng	Tổng Giám Đốc
Head of Information Security	*Chief Technology Officer*	*General Counsel*	*Chief Executive Officer*

I. Phạm Vi Điều Chỉnh, Mục Đích Và Đối Tượng Áp Dụng

Scope, Purpose And Regulated Entities

1. Phạm vi điều chỉnh / *Scope*

- **Chính Sách An Ninh Thông Tin** ("Chính sách") áp dụng trong Công ty Cổ phần Tập đoàn Masan, các Công ty thành viên (hiện hữu hoặc thành lập mới, mua bán, sáp nhập trong tương lai), các Công ty liên kết do Công ty Cổ phần Tập đoàn Masan hoặc Công ty thành viên quản lý, chi phối hoặc nắm quyền kiểm soát (gọi riêng là "Công ty", gọi chung là "Tập đoàn Masan" hoặc "Masan").

  Information Security Policy *("Policy") shall apply to Masan Group Corporation, its Member Companies (existing or newly established, acquired, or merged in the future), Affiliated Companies managed, influenced, or controlled by Masan Group Corporation or its Member Companies (referred to individually as the "Company", collectively as "Masan Group" or "Masan").*

2. Mục đích / *Purpose*

Chính sách này ban hành nhằm / *The Policy is issued to:*

- thiết lập các quy định về việc đảm bảo an toàn thông tin, sử dụng, khai thác và bảo mật Hệ thống thông tin Masan;

  set out regulations for ensuring the information security, use, exploitation and protection of the Masan's Information System;

- thống nhất chính sách an ninh thông tin cho tất cả các Công ty trực thuộc Masan; *establish unified information security policies for all Masan's Companies;*
- mô tả Hệ thống thông tin Masan;

  describe the Masan's Information System;

- truyền đạt các chính sách của Hệ thống thông tin và các quá trình cũng như các yêu cầu cần thiết hỗ trợ cho Hệ thống này;

  communicate the policies of the Information System and the necessary supporting processes and requirements for this System;

- xác định các tiêu chuẩn quốc tế sẽ sử dụng trong Hệ thống thông tin;

identify international standards to be used in the Information System;

- kiểm soát các hoạt động và việc thực hiện Hệ thống thông tin;
  control activities and implementing the Information System;
- đưa ra các chỉ dẫn về việc thực hiện Hệ thống thông tin Masan.
  provide guidelines for implementing Masan's Information System.

3. Đối tượng áp dụng / *Entites*

Các quy định tại Chính sách này áp dụng đối với / *The provisions of the Policy apply to:*

- các Hệ thống thông tin Masan;
  Masan's information systems;
- các dữ liệu được kiểm soát, xử lý trong Masan và/hoặc Hệ thống thông tin Masan;
  all data controlled, processed in Masan and/or Masan's information systems;
- các Bộ phận/cá nhân quản lý và vận hành các Hệ thống thông tin Masan;
  departments/individuals managing and operating Masan's information systems;
- người dùng, Đối tác, khách hàng, Bên thứ ba sử dụng, khai thác Hệ thống thông tin Masan;
  users, partners, customers, third parties using and exploiting Masan's information systems.

II. Nguyên Tắc Chung / *General Principles*

- Tuân thủ theo các yêu cầu của Luật an toàn thông tin mạng và các quy định hiện hành có liên quan;
  Comply with the requirements of the Cyber Information Security Law and relevant applicable regulations;
- Thông tin phải đảm bảo tính bảo mật, tính toàn vẹn và và tính sẵn sàng cho mục đích công việc;
  Information must be confidentiality, integrity and availibility for work purposes;
- Truy cập thông tin theo đúng chức năng, nhiệm vụ, quyền hạn. Việc truy cập thông tin phải được kiểm soát đảm bảo ngăn chặn các truy cập trái phép;
  Access to information should be based on function, duty and authority. To access information must be controlled to ensure the prevention of unauthorized access;
- Nhân viên Công ty phải có trách nhiệm tuân thủ và đảm bảo an toàn thông tin theo phạm vi hoạt động;
  All employees are responsible for complying with and ensuring information security within their scope of activities;
- Tất cả các vi phạm về an ninh thông tin phải được xem xét, điều tra và xử lý theo quy định của Masan.
  All violations of information security must be reviewed, investigated and handled according to Masan's regulations.

III. Định Nghĩa / *Definition*

1. **Bộ phận:** được hiểu là ban/phòng ban đảm nhiệm lĩnh vực chuyên môn nhất định; có cơ cấu tổ chức, quyền hạn và trách nhiệm cụ thể nhằm đảm bảo chức năng quản trị và muc tiêu đề ra.

Department: *means that a sector / department is responsible for specific specialized fields; with specific organizational structure, authority and responsibility to ensure administrative and target-setting functions.*

2. **Bí mật chứng thực:** là thông tin nhạy cảm như Mật khẩu, mã PIN hoặc khóa bảo mật, được sử dụng để xác minh danh tính và cấp quyền truy cập trong các hệ thống bảo mật, và được xem là thông tin mật của Công ty.

   Authentication secrets*: are sensitive information such as passwords, PIN codes, or security keys, used to verify identity and grant access within security systems, and are considered Confidential information of Masan.*

3. **Công ty thành viên:** là công ty mà Công ty trong Tập đoàn Masan nắm trực tiếp hoặc gián tiếp từ 50% vốn điều lệ trở lên.

   Member Company*: a company in which a Company within Masan directly or indirectly holds more than 50% of its charter capital.*

4. **Công ty liên kết**: là công ty được Công ty trong Tập đoàn Masan nắm trực tiếp hoặc gián tiếp từ 20% vốn điều lệ trở lên

   Affiliated Company*: a company in which a Company within the Masan Group directly or indirectly holds 20% or more of its charter capital.*

5. **Đối tác:** là cá nhân, tổ chức cung cấp hàng hóa, dịch vụ cho Công ty và/hoặc mua, sử dụng hàng hóa, dịch vụ của Công ty và/hoặc hợp tác với Công ty về một công việc cụ thể thông qua việc xác lập thỏa thuận / hợp đồng với Công ty.

   Partner*: is an individual or organization that provides goods and services to the Company and/or purchases, uses the Company's goods and services and/or cooperates with the Company on a specific project through an agreement / contract with the Company.*

6. **Downtime:** là thời gian ngừng hoạt động.

   Downtime: *means the period when operations are suspended.*

7. **Dữ liệu / Thông tin:** là tất cả các thông tin có giá trị đối với Công ty / Masan liên quan đến, bao gồm nhưng không giới hạn, công nghệ, ý tưởng, kiến thức, quy trình, sáng chế, bí mật kinh doanh, thiết kế, nghiên cứu, phương pháp kinh doanh, hoạt động kinh doanh, thông tin tài chính, các kế hoạch sản xuất, các kế hoạch tiếp thị và/hoặc cách tiếp cận, dưới dạng văn bản, hồ sơ, hình ảnh hoặc bất kỳ định dạng nào khác.

   Data / Information: *includes all information valuable to Masan related to, including but not limited to, technology, ideas, knowledge, processes, inventions, trade secrets, designs, research, business methods, business activities, financial information, production plans, marketing plans, and/or approaches, in the form of documents, records, images, or other formats.*

8. **Dữ liệu nhạy cảm:** là dữ liệu có thông tin Mật, thông tin Nội bộ của Công ty và/hoặc do Công ty quản lý, nếu bị tiết lộ ra ngoài trái quy định sẽ gây ảnh hưởng xấu đến danh tiếng, tài chính và hoạt động của Công ty và/hoặc của cổ đông, Đối tác và khách hàng của Công ty.

   Sensitive Data: *means that Confidential, internal information, if disclosed, can have adverse effects on prestige, finance or business of Company and/or its shareholders, Partners, or customers.*

9. **Giải mã dữ liệu:** là một quy trình ngược lại với quá trình mã hóa để khôi phục dữ liệu gốc như trước khi nó được mã hóa.

Data decryption: *a program that reverses the encryption process to restore the original data before it was encrypted.*

10. **Hệ thống:** là phần mềm dùng để tổ chức và duy trì hoạt động của một hệ thống hoặc một thiết bị số (sau đây gọi chung là thiết bị số). Phần mềm hệ thống có thể tạo môi trường cho các phần mềm ứng dụng làm việc trên đó và luôn ở trạng thái làm việc khi thiết bị số hoạt động.

    System: *is software used to organize and maintain the operation of a system or digital device. System software can create an environment for application software to work on and is always in a working state when the digital device is operating.*

11. **Hệ thống an ninh mạng:** là tập hợp các thiết bị tường lửa; thiết bị kiểm soát, phát hiện truy cập bất hợp pháp; phần mềm quản trị, theo dõi, ghi nhật ký trạng thái an ninh mạng và các trang thiết bị khác có chức năng đảm bảo an toàn hoạt động của mạng, tất cả cùng hoạt động đồng bộ theo một chính sách an ninh mạng nhất quán nhằm kiểm soát chặt chẽ tất cả các hoạt động trên mạng.

    Network security system: *means that a collection of firewall devices; unauthorized access control and detection devices; management software, monitoring, logging network security status and other devices with functions to ensure the safe operation of the network, all operating synchronously under a consistent network security policy to tightly control all activities on the network.*

12. **Hệ thống thông tin:** là một tập hợp có cấu trúc các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu, hệ thống mạng và hạ tầng hệ thống điện toán đám mây phục vụ cho một hoặc nhiều hoạt động kỹ thuật, nghiệp vụ của Công ty và/hoặc Masan.

    Information system: *means that a structured collection of hardware devices, software, databases, network systems, cloud infrastructures serving one or more technical and business of Company and/or Masan.*

13. **Internet:** là một hệ thống gồm các mạng máy tính được liên kết với nhau trên phạm vi toàn thế giới, tạo điều kiện thuận lợi cho các dịch vụ truyền thông dữ liệu, như đăng nhập từ xa, truyền các tệp tin, thư tín điện tử, và các nhóm thông tin. Internet là một phương pháp ghép nối các mạng máy tính hiện hành, phát triển một cách rộng rãi tầm hoạt động của từng hệ thống thành viên.

    Internet: *means that a system consisting of interconnected computer networks worldwide, facilitating convenient data communication services such as remote login, file transmission, email, and information groups. The Internet is a method of connecting existing computer networks, expanding the operational scope of each member system.*

14. **ISO (Information Security Office):** Bộ phận An toàn thông tin – Công ty cổ phần Tập đoàn Masan.

    ISO (Information Security Office): *The Information Security Department - Masan Group Corporation.*

15. **IT (Information Technology):** Bộ phận IT / Tech của Công ty.

    IT (Information Technology): *The IT / Technology Department of Company.*

16. **Mã hóa dữ liệu:** là việc sử dụng một chương trình có thuật toán đặc biệt để thay đổi cách thể hiện dữ liệu.

    Data encryption: *means that the use of a program with a special algorithm changes the representation of data.*

17. **Malware:** là phần mềm độc hại được thiết kế để gây hại cho hệ thống máy tính hoặc mạng.

***Malware**: means that a malicious software is designed to harm a computer system or network.*

18. **Mật khẩu:** là một dãy các ký tự nhằm để xác thực quyền truy cập vào một hệ thống hoặc chứng thực một sự kiện nào đó, và chỉ người được cấp mât khẩu mới biết và có quyền thay đổi Mật khẩu.

    ***Passwords:** means that a series of characters used to authenticate access rights to a system or verify a certain event, and only authorized individuals know it and have the right to change it.*

19. **Ngôn ngữ kích động:** là bất kỳ hình thức biểu đạt nào gây thù hận, bạo lực hoặc phân biệt đối xử đối với một cá nhân hoặc nhóm người dựa trên các đặc điểm như chủng tộc, tôn giáo, giới tính, khuynh hướng tình dục, hoặc quốc tịch.

    ***Inflammatory language:** any form of expression that generates hatred, violence, or discrimination against an individual or group based on attributes such as race, religion, gender, sexual orientation, or nationality.*

20. **Người quản trị hệ thống**: là người chịu trách nhiệm quản lý, vận hành và duy trì hoạt động hệ thống thông tin.

    ***System Administrator:** means that a person is responsible for managing, operating and maintaining an information system.*

21. **Người sở hữu thông tin:** là người chịu trách nhiệm về tính toàn vẹn và thống nhất của thông tin, người có thể thêm, xóa, sửa thông tin.

    ***Information Owner**: means that a person is responsible for the integrity and consistency of information and can add, delete, and modify such information.*

22. **Nhà cung cấp:** là Đối tác cung cấp hàng hóa, dịch vụ cho Công ty.

    ***Supplier**: means Partner that provides goods or services to Company.*

23. **Quy định nội bộ**: là hệ thống tất cả và/hoặc bất kỳ nội quy, chính sách, quy định, quy trình, quy chế, hướng dẫn, thông báo và/hoặc bất kỳ tài liệu nào được ban hành dưới hình thức văn bản và/hoặc điện tử trong phạm vi áp dụng của Công ty và/hoặc Tập đoàn Masan liên quan đến an ninh thông tin.

    ***Internal Regulations:** refers to the system of all and/or any internal rules, policies, regulations, procedures, guidelines, notifications, and/or any documents issued in written and/or electronic format within the scope of application of the Company and/or Masan Group related to the information security.*

24. **Ransomware:** là loại malware mã hóa dữ liệu của nạn nhân và yêu cầu tiền chuộc để khôi phục quyền truy cập.

    ***Ransomware:** means that a type of malware encrypts the victim's data and demands a ransom to restore access.*

25. **Tài sản:** là tất cả các tài nguyên vật chất và phi vật chất thuộc sở hữu hoặc quản lý của Công ty, bao gồm thiết bị, cơ sở hạ tầng, thông tin, tài sản trí tuệ, Hệ thống thông tin và tài liệu.

    ***Assets:** includes all tangible and intangible resources owned or managed by Company, encompassing equipment, infrastructure, information, intellectual property, Information Systems and documents.*

26. **Thiết bị lưu điện (UPS):** là thiết bị được dùng để tích trữ điện và chúng được dùng khi nguồn điện chính bị ngắt. Hầu hết các UPS còn có tính năng chống sốc điện.

Uninterruptible Power Supply (UPS): *means that a device is used to store electricity and is activated when the main power source is interrupted. Most UPS devices also have surge protection features.*

27. **Thư điện tử (e-mail):** là ứng dụng mạng diện rộng mà trong đó thư điện tử là những tín hiệu điện mang các thông điệp, được truyền giữa những người sử dụng, thông qua mạng máy tính, internet và sử dụng nhiều các nghi thức mạng khác nhau.

    Email: *means that a wide-area network application in which email is electrical signals carrying messages, transmitted between users, through computer networks, the internet and using various network protocols.*

28. **Tin tặc:** là hành động / chủ thể xâm nhập bất hợp pháp vào một hệ thống máy tính. ***Hackers:*** *means that an act / object illegally infiltrates a computer system.*

29. **Trang chủ:** là một dạng siêu văn bản được dùng để công bố thông tin trên mạng Internet.

    Homepage*: means that a type of hypertext is used to publish information on the wide Internet.*

30. **Ứng dụng:** là phần mềm được phát triển và cài đặt trên một môi trường nhất định, nhằm thực hiện những công việc, những tác nghiệp cụ thể.

    Application: *is software developed and installed in a certain environment, to perform specific tasks and operations.*

31. **Virus:** là một chương trình máy tính có khả năng tự nhân bản, có khả năng phá hủy, hoặc là nguyên nhân gây lên sự trục trặc của một hệ thống máy tính mà nó lây nhiễm vào. ***Virus:*** *means that a computer program is capable of self-replication and has the ability to destroy or cause disruptions in an infected computer system.*

32. **WWW (World Wide Web):** gọi tắt là Web hoặc WWW, là một không gian thông tin toàn cầu mà mọi người có thể truy cập (đọc và viết) qua các máy tính nối với mạng Internet.

    WWW (World Wide Web): *also known as the Web or WWW, is a global information space that people can access (read and write) through computers connected to the Internet.*

IV. Quy Định Cụ Thể / *Specific Regulations*

Xem Quy định An toàn thông tin đính kèm *(Please find Information Security Regulations as attached)*

V. Điều Khoản Khác / *Miscellaneous*

- Chính sách này có hiệu lực thi hành kể từ Ngày hiệu lực và có thể được sửa đổi, cập nhật tùy từng thời điểm.

  This Policy comes into force from the Effective Date and may be amended, updated from time to time.

- Chính sách này nên được đọc cùng với các Quy định nội bộ có liên quan của Công ty.

  This Policy should be read in conjunction with the Company's relevant Internal Regulations.

- Các vấn đề chưa được đề cập cụ thể trong Chính sách này sẽ tuân thủ theo Quy định nội bộ (nếu có) và/hoặc quy định pháp luật liên quan và/hoặc hướng dẫn, điều phối từ Bộ phận ISO và/hoặc IT.

Terms not specifically addressed in this Policy shall adhere to the Company's Internal Regulations (if any), and/or applicable law, and/or guidance and coordination from ISO / IT Department.

- Nhân viên các cấp (đang làm việc hoặc đã nghỉ việc, dưới bất kỳ hình thức quan hệ lao động nào, đã ký hoặc chưa ký hợp đồng lao động) thuộc các bộ phận/phòng ban liên quan có trách nhiệm chấp hành nghiêm chỉnh Chính sách này, nếu vi phạm thì tùy theo tính chất, mức độ vi phạm sẽ bị xử lý theo quy định của pháp luật, Quy định nội bộ của Công ty và/hoặc Tập đoàn Masan.

  Employees at all levels (currently employed or resigned, under any form of labor relations, whether contracts are signed or not) of the relevant departments/divisions are responsible for strict compliance with this Policy. Violations, depending on their nature and severity, will be handled according to applicable law, the Company's Internal Regulations, and/or the policies of Masan Group.

- Chính sách này được soạn thảo song ngữ Việt - Anh. Trong trường hợp có sự mâu thuẫn, điều khoản tiếng Việt sẽ có giá trị ưu tiên áp dụng.

  This Policy is drafted bilingually in Vietnamese - English. In case of any inconsistency, the Vietnamese language terms shall prevail.

VI. Văn Bản Liên Quan / *Related Documents*

STT *No.*	**Tên văn bản** *Document name*	**Số văn bản** *Document No.*	**Ngày ban hành** *Date of issuance*
Văn bản bên ngoài / *External Documents*			
1	Luật An Ninh Mạng *Cyber Security Law*	24/2018/QH14	12/06/2018
2	Luật An toàn thông tin Mạng *Cyberinformation Security Law*	86/2015/QH13	19/11/2015
3	Luật Dân Sự *Civil Code*	91/2015/QH13	24/11/2015
4	Nghị Định Bảo Vệ Dữ Liệu Cá Nhân *Personal Data Protection Decree*	13/2023/NĐ-CP	17/04/2023
5	Hệ thống An toàn Thông tin ISO/IEC 27001:2022 *ISO/IEC 27001:2022 Information Security System*	N/A	10/2022
Văn bản nội bộ / *Internal Documents:*			
1	Chính sách Quản lý Dữ liệu Cá Nhân *Personal Data Management Policy*	MSN-PL-CS-01	01/03/2024

VII. Lịch sử tài liệu / *Version History*

Phiên bản *Version*	**Nội dung thay đổi** *Changelog*	**Ngày phê duyệt** **Approved Date**
1.0	Văn bản ban đầu *Initial Document*	01/07/2024

QUY ĐỊNH AN TOÀN THÔNG TIN
INFORMATION SECURITY REGULATIONS

ĐIỀU 1. QUY ĐỊNH VỀ QUYỀN TRUY CẬP VÀ SỬ DỤNG INTERNET, EMAIL
ARTICLE 1. REGULATIONS ON ACCESS AND USE OF INTERNET, EMAIL

1. Quy tắc chung / *General Rules*

- Khi có nhu cầu truy cập Internet để tham khảo, tra cứu, cập nhật các thông tin, tài liệu và/hoặc sử dụng email cho mục đích công việc cho Công ty, nhân viên sử dụng Internet, Email một cách hiệu quả, tuân thủ quy định pháp luật và Quy định nội bộ của Công ty. Việc không tuân thủ các quy định này sẽ là căn cứ để từ chối quyền truy cập và/hoặc áp dụng các hình thức kỷ luật khác.

  Accessing the Internet to research, look up, update information, documents and/or using email for Company's business, it is the responsibility of employees to use Internet, Email effectively, comply with the law and Internal Regulations. Failure to comply with these provisions may result in denial of access or other disciplinary measures.

2. Quyền truy cập / *Access rights*

- Việc đăng ký tài khoản, quyền truy cập mới cho nhân viên hoặc thiết bị sử dụng mạng nội bộ phải được phê duyệt có nêu rõ mục đích sử dụng và được sự đồng ý của giám đốc Bộ phận.

  New account, access rights registration for employees or devices using the internal network must be approved with a clear purpose and the consent of the Department director.

- Các nhân viên không được chia sẻ tài khoản của mình cho người khác, trừ trường hợp tài khoản đó được lập ra cho mục đích dùng chung và được phê duyệt. Nhân viên phải chịu trách nhiệm trong việc người khác có thể chiếm Mật khẩu nếu sử dụng chung tài khoản.

  Employees are not allowed to share their accounts, except when the account is created for shared use and approved. Employees are responsible for the security of their Passwords if using a shared account.

- Nghiêm cấm việc cố tình truy cập bằng tài khoản của người khác.

  Deliberately accessing someone else's account is strictly prohibited.

3. Truy cập và sử dụng Internet, Email / *Accessing and using Internet, Email*

- Tất cả nhân viên sẽ được cấp một tài khoản email thuộc Công ty, và tài khoản này chỉ được sử dụng khi thực hiện các công việc cho Công ty. Nhân viên không được phép chuyển tiếp email của Công ty đến tài khoản email cá nhân.

  All employees will be provided with a Company email account, which should be used when performing tasks for Company. Employees are not allowed to forward Company emails to personal email accounts.

- Khi cần gửi thông tin mang tính bảo mật qua email, hãy dùng tệp đính kèm được bảo vệ bằng Mật khẩu.

  When sending confidential information via email, use password-protected attachments.

- Không xem, hiển thị, lưu trữ hoặc chuyển tiếp các nội dung (bao gồm văn bản và hình ảnh) mà có thể được coi là khiêu dâm, phân biệt chủng tộc, phân biệt giới tính hoặc phản cảm.

  Do not view, display, store or forward content (including text and images) that can be considered as pornography, racial discrimination, gender discrimination or offensive.

- Tất cả các email nên giới hạn trên một màn hình văn bản nếu có thể. Không đính kèm file lớn hơn 25MB.

  All emails should be limited to one text screen if possible. Do not attach files larger than 25MB.

- Không sử dụng ngôn ngữ kích động.

  Do not use inflammatory language.

- Hành xử văn minh và tôn trọng khi tương tác với những người sử dụng Internet khác.

  Behave with cultural respect towards other Internet users.

4. **Hoạt động bị cấm trên Internet (trong thời gian làm việc) / *Activities are prohibited on the Internet (during working hours)***

- Không tham gia bất hợp pháp vào các ứng dụng Internet nhiều người dùng và tất cả các trò chơi trên Internet;

  Do not engage in illegal activities on multi-user Internet applications and all online games;

- Không sử dụng các ứng dụng trò chuyện/mạng xã hội (Chat) nằm trong Danh sách phần mềm Blacklist trên thiết bị của Công ty, ngoại trừ trường hợp có sự phê duyệt của trưởng Bộ phận;

  Do not use Chat programs listed in the Blacklist on Company devices unless approved by Department head;

- Không sử dụng email cá nhân, các nền tảng lưu trữ cá nhân khác.

  Do not use personal email, other personal storage platforms.

5. **Hoạt động bất hợp pháp / *Engaging in illegal activities***

- Không cài đặt sử dụng các phần mềm, lưu trữ các tài liệu không có bản quyền trong hệ thống, thiết bị của Công ty; tuân thủ các yêu cầu về bản quyền phần mềm.

  Do not install or use unlicensed software, and do not store copyrighted documents on company systems or devices; comply with all software copyright requirements.

- Không được thực hiện việc phát tán có chủ ý các loại virus vào bất cứ hệ thống nào, hoặc gắn kết với bất kỳ chương trình nào của tội phạm công nghệ.

  Do not intentionally distribute any type of virus to any system or associate with any criminal technology program.

- Không tuyên truyền, kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, thuần phong mỹ tục của dân tộc.

  Do not promote or incite violence, obscenity, depravity, crimes, social vices, superstitions, cultural destruction, or national customs.

- Không tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác do pháp luật quy định.

  Do not disclose state secrets, military secrets, security, economic, diplomatic secrets, and other secrets as stipulated by law.

- Không đưa thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân.

  Do not spread distorted information, fabrications, or insult the reputation of organizations, honor and dignity of individuals.

- Không quảng cáo, tuyên truyền, mua bán hàng hóa, dịch vụ bị cấm; truyền bá tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm bị cấm.

Do not advertise, promote, trade prohibited goods and services; propagate press works, literature, art, banned publications.

- Không giả mạo tổ chức, cá nhân và phát tán thông tin giả mạo, thông tin sai sự thật xâm hại đến quyền và lợi ích hợp pháp của tổ chức, cá nhân.

  Do not impersonate organizations or individuals and disseminate false information that harms the legal rights and interests of organizations and individuals.

- Không tạo đường dẫn trái phép đối với tên miền hợp pháp của tổ chức, cá nhân; tạo, cài đặt, phát tán phần mềm độc hại, vi-rút máy tính; xâm nhập trái phép, chiếm quyền điều khiển hệ thống thông tin, tạo lập công cụ tấn công trên Internet; sử dụng mạng Công ty để thực hiện hành vi tấn công an ninh mạng trái quy định pháp luật (tham chiếu Luật An ninh mạng). Điều này không áp dụng với Bộ phận ISO khi thực hiện các hoạt động kiểm tra an ninh, an toàn thông tin được cấp có thẩm quyền phê duyệt.

  Do not create unauthorized links to the legitimate domain names of organizations or individuals; do not create, install, or distribute malicious software, computer viruses; do not intrude unlawfully or take control of information systems, and do not develop internet attack tools; do not use the Company's network to carry out illegal cybersecurity attacks (refer to the Cybersecurity Law). This regulation does not apply to the ISO Department when carrying out security and information security assessment approved by competent authorities.

6. **Danh sách phần mềm Blacklist:** Zalo, Viber, Whatsapp, Messenger, Telegram, Discord, WeChat. *Blacklist software: Zalo, Viber, Whatsapp, Messenger, Telegram, Discord, WeChat.*

ĐIỀU 2. CHẤP NHẬN SỬ DỤNG TÀI SẢN

ARTICLE 2 ACCEPTANCE OF ASSET USE

1. **Nhận thức chung / *General awareness***

   - Tất cả nhân viên đọc, hiểu và quen thuộc với các Quy định nội bộ liên quan của Công ty và/hoặc Masan;

     All employees read, understand and are familiar with Internal Regulations of Masan and/or Company;

   - Tham dự đầy đủ các khóa hướng dẫn về An toàn thông tin bắt buộc theo sự phân công của cấp quản lý;

     Attend all mandatory Information Security training sessions as assigned by management;

   - Không sử dụng bất kỳ thông tin, dữ liệu liên quan đến hoặc phát sinh từ Công ty mà không nhằm mục đích hoạt động kinh doanh của Công ty (như sử dụng cho mục đích cá nhân);

     Do not use any information, data related to or arising from Company for purposes other than the company's business (such as personal use);

   - Không sử dụng các thông tin với bản quyền hoặc quyền sở hữu trí tuệ thuộc sở hữu của bên thứ ba; *Do not use copyrighted or intellectual property information owned by third parties;*

   - Thông báo ngay cho quản lý hoặc Bộ phận ISO / IT khi phát hiện có vi phạm hoặc nghi ngờ có vi phạm chính sách an toàn thông tin, các sự cố an ninh (chẳng hạn như việc rò rỉ các thông tin bảo mật của Công ty);

     Immediately notify your manager or ISO / IT Department when detecting or suspecting violations of information security policies, security incidents (such as leaking company's confidential information);

- Không click vào các đường dẫn (link) lạ, không mở các file đính kèm nghi ngờ. Kiểm tra kĩ đường link, file đính kèm và xác nhận lại nếu thấy nghi ngờ;

  Do not click on suspicious links, do not open suspicious attachments. Check the link and attachment carefully and confirm if in doubt;

- Không chuyển tiếp các email vi phạm các quy định trong Điều 1 và / hoặc chứa thông tin nhạy cảm.

  Do not forward emails that violate the regulations in Article 1 and /or contain sensitive information.

2. Truy cập và sử dụng hệ thống CNTT / *Access and use IT systems*

- Công nhận rằng việc sử dụng hệ thống máy tính của Công ty có thể được giám sát truy cập vào mạng nội bộ và Internet, hoặc/và ghi nhật ký lại cho các mục đích hợp pháp;

  Acknowledge that the use of Company's computer system may be monitored for access to internal and Internet networks and/or recorded for legitimate purposes;

- Không truy cập các dữ liệu nhạy cảm khi chưa được phép, không lạm dụng quyền để thực hiện các hành động gây tổn hại cho Công ty;

  Do not access sensitive data without permission, do not abuse rights to perform actions that harm the Company;

- Nhân viên sẽ chịu trách nhiệm về việc sử dụng và bảo vệ thông tin xác thực mà mình được cung cấp;

  Employees are responsible for using and protecting the provided authentication information;

- Khi bị lộ quyền truy cập vào các công cụ, ứng dụng với bất kỳ lý do gì, nhân viên phải thay đổi Mật khẩu ngay lập tức và thông báo đến các Bộ phận liên quan (IT, ISO, v.v.) để được trợ giúp và xử lý;

  When access rights to tools, applications are compromised for any reason, employees must immediately change their passwords and report to relevant Departments (IT, ISO, etc.) for assistance and resolution;

- Đăng xuất khỏi mạng, công cụ, ứng dụng khi không có nhu cầu sử dụng;

  Log out of the network, tools, applications when not in use;

- Không sử dụng các thiết bị lưu trữ di động cá nhân, máy tính cá nhân để lưu trữ các dữ liệu nhạy cảm của Công ty;

  Do not use personal mobile storage devices and laptop to store the Company's sensitive data;

- Tắt hoặc khóa máy tính khi rời khỏi văn phòng;

  Turn off or lock your computer when leaving the office;

- Trách nhiệm của nhân viên và những người có đặc quyền sử dụng VPN phải đảm bảo rằng những người sử dụng trái phép không được phép truy cập vào mạng nội bộ Công ty thông qua tài khoản VPN của mình.

  The responsibility of employees and VPN privileged users is to ensure that unauthorized users are not allowed to access the Company internal network through their VPN accounts.

3. Bảo vệ tài sản Công ty / *Protect Company assets*

- Nhân viên sẽ bảo vệ mọi loại Thông tin mình gửi, nhận, lưu trữ, xử lý tương ứng với mức độ phân loại Thông tin, kể cả bản giấy lẫn điện tử;

Employees shall protect all types of information they send, receive, store, and process according to the level of classification, including both paper and electronic documents;

- Không gửi Thông tin mang tính Mật qua các phương thức công cộng như Wifi, Internet, Email công cộng trừ phi đã áp dụng biện pháp thích hợp để bảo vệ Thông tin đó khỏi sự truy cập trái phép (ví dụ: mã hóa);

  Do not send Confidential Information through public methods such as Wi-Fi, Internet, public email unless appropriate measures are applied to protect that information from unauthorized access (e.g., encryption);

- Nhân viên sẽ lưu trữ an toàn tài liệu, dữ liệu và thông tin Mật, thông tin Nội bộ và đảm bảo nó được tiêu hủy đúng đắn khi không còn cần thiết;

  Employees will securely store Confidential documents / information / data and ensure their proper destruction when no longer needed;

- Áp dụng các biện pháp phòng ngừa để bảo vệ laptop và thiết bị di động khi mang chúng bên ngoài Công ty;

  Apply preventive measures to protect laptops and mobile devices when taking them outside of Company;

- Chịu trách nhiệm cập nhật bản vá lỗi, duy trì giải pháp chống phần mềm độc hại trên các thiết bị mình có quyền quản trị;

  Responsible for updating patches, maintaining anti-malware solutions on their managed devices;

- Ngắt kết nối máy tính xách tay / máy tính để bàn ra khỏi mạng của Công ty khi bị nhiễm (hoặc nghi ngờ có) phần mềm độc hại, và ngay lập tức liên hệ với Bộ phận IT để được hướng dẫn;

  Disconnect the laptop / desktop from the Company's network when infected (or suspected to be infected) with malware, and immediately contact the IT Department for guidance;

- Đối với các cá nhân sử dụng máy tính/thiết bị công nghệ thông tin chứa các dữ liệu quan trọng, cần bảo mật thông tin của Công ty, ngoài bắt buộc thực hiện các yêu cầu trên phải được cài đặt thêm 2 yêu cầu bên dưới này:

  For individuals using computers/IT devices containing important data that needs to be protected by the Company, in addition to mandatory requirements, the following two additional requirements must be implemented:

  - Mã hóa dữ liệu trên các thiết bị lưu trữ (ổ cứng, usb,…);

    Encrypt data on storage devices (hard drives, USBs, etc.);

  - Phải thiết lập bảo vệ phần cứng thiết bị khi khởi động máy (Mật khẩu Bios, Mật khẩu ổ cứng).

    Set up hardware protection for devices during startup (BIOS password, hard drive password).

4. Không gian làm việc an toàn / *Safe working space:*

- Tài liệu, hồ sơ bản cứng có chứa Thông tin Mật phải được cất giữ an toàn khi không dùng đến;

  Hard copy documents/files containing Confidential Information must be securely stored when not in use;

- Tủ hồ sơ chứa Thông tin Mật phải luôn được đóng và khóa khi rời khỏi văn phòng. *Filing cabinets containing Confidential Information must always be closed and locked when leaving the office.*

- Văn bản giấy trước khi hủy hay bỏ vào thùng rác cần xem xét lại nội dung và phải đảm bảo không

thể khôi phục được nếu chứa Thông tin Mật.

Before disposing or putting paper documents into the trash, review the content and ensure it cannot be recovered if it contains Confidential Information.

- Thiết bị được sử dụng để lưu trữ và/hoặc xử lý thông tin Mật phải được khóa và cất giữ an toàn khi không sử dụng.

  Devices used to store and/or process Confidential information must be locked and securely stored when not in use.

- Không mở Thông tin Mật trên màn hình máy tính mà không có sự trông coi. *Do not display Confidential Information on a computer screen without supervision.*
- Đăng xuất (log-off) ứng dụng hoặc kết thúc phiên làm việc sau khi kết thúc công việc với ứng dụng/ hệ thống;

  Log off applications or end work sessions after completing tasks with applications/systems;

- Không mô tả cho người ngoài về các khu vực làm việc trong Công ty;

  Do not describe work areas within the Company to outsiders;

- Không mở cửa cho người lạ vào khu vực làm việc trong Công ty;

  Do not open the door for strangers to enter work areas within the company;

- Xóa bảng sau khi hoàn tất buổi họp.

  Erase the whiteboard after completing a meeting.

ĐIỀU 3 QUY ĐỊNH PHÂN LOẠI MỨC ĐỘ QUAN TRỌNG CỦA THÔNG TIN, HỆ THỐNG VÀ ỨNG DỤNG

ARTICLE 3 CLASSIFICATION OF INFORMATION, SYSTEMS AND APPLICATIONS LEVELS

1. Phân loại mức độ quan trọng của thông tin / *Classification levels of information:*

- Thông tin phải được phân loại theo 3 mức độ riêng biệt: Mật, Nội bộ và Không phân loại. Các mức độ được định nghĩa như sau:

  Information must be classified into 3 distinct levels: Confidential, Internal Use Only, and Unclassified. The levels are defined as follows:

  - **MẬT:** cấp độ này áp dụng cho các thông tin kinh doanh nhạy cảm chỉ dùng trong nội bộ của Công ty. Việc tiết lộ những thông tin này cho những người không có thẩm quyền có thể gây nguy hại đặc biệt nghiêm trọng cho Công ty, các cổ đông, các đối tác kinh doanh, hoặc khách hàng của Công ty, bao gồm: ảnh hưởng đến các mục tiêu tổng quan của Công ty, tiết lộ/mất/thay đổi dữ liệu người dùng, gây tổn hại đến uy tín, gây ra thiệt hại tài chính, tạo ra các rủi ro/trách nhiệm pháp lý. Thông tin Mật bao gồm nhưng không giới hạn như thông tin có tiềm năng cung cấp lợi thế cạnh tranh, thông tin liên quan đến sự vi phạm hoặc được cho là vi phạm, thông tin hoạch định chiến lược, thông tin về sáp nhập, mua lại, dự báo hoặc kết quả tài chính, thông tin khách hàng (Thông tin định danh cá nhân của khách hàng, thông tin giao dịch), Mật khẩu, khóa mã hóa và bí mật chứng thực. Tất cả các bản in, viết tay, những vật hiển thị các thông tin mật phải được đóng dấu / gắn nhãn "MẬT" / "CONFIDENTIAL" trên góc trái / phải phía trên / dưới của trang giấy hoặc các thông tin, tài liệu về mặt bản chất hoặc bối cảnh phải được xem / hiểu là thông tin Mật thì việc sử dụng các thông tin này phải được sự cho phép của cấp quản lý có thẩm quyền.

- *CONFIDENTIAL: This classification level is applied to sensitive business information used internally within the Company. Disclosure of this information to unauthorized persons could cause particularly severe harm to the Company, its shareholders, business partners, or customers, including affecting the company's overall objectives, disclosing/losing/altering user data, damaging reputation, causing financial loss, and creating legal risks/liabilities. Confidential information includes but is not limited to information that provides a competitive edge, information related to actual or alleged breaches, strategic planning information, details about mergers and acquisitions, financial forecasts or outcomes, customer information (Personal Identifiable Information of customers, transaction information), passwords, encryption keys, and authentication secrets. All printed or handwritten materials displaying confidential information must be stamped or labeled with "MẬT" / "CONFIDENTIAL" on the upper/lower left/right corner of the page. Any information or documents that are inherently or contextually deemed confidential must be treated accordingly, and their use must be authorized by the appropriate management level.*
- **NỘI BỘ:** cấp độ này áp dụng cho các thông tin chỉ dùng trong nội bộ Công ty, Công ty thành viên, Công ty liên kết hay Đối tác, Bên thứ ba, được phân quyền quản lý, khai thác cho một hoặc một nhóm đối tượng được xác định danh tính. Việc tiết lộ những thông tin này cho những người không có thẩm quyền sẽ vi phạm các điều luật, quy định, thỏa thuận với Đối tác, Bên thứ ba hoặc gây nguy hại nghiêm trọng cho Công ty, khách hàng hay Đối tác, Bên thứ ba, bao gồm: thay đổi mục tiêu kinh doanh của Công ty, gây tổn hại đến danh tiếng của Công ty. Thông tin Nội bộ bao gồm nhưng không giới hạn như báo cáo kiểm toán nội bộ và độc lập, đánh giá an ninh, đánh giá tuân thủ hoặc báo cáo đảm bảo, tài liệu nội bộ, thông tin nhân viên (lương, thưởng, v.v.), thông tin liên lạc nội bộ (Thông tin định danh cá nhân của Nhân viên dành cho mục đích liên hệ trong Công ty), thông tin mô hình, cấu trúc, công nghệ, v.v. mà công ty đang sử dụng. Tất cả các bản in, viết tay, những vật hiển thị các thông tin nội bộ phải được đóng dấu/ gắn nhãn "NỘI BỘ" / "INTERNAL USE ONLY" trên góc trái / phải phía trên / dưới của trang giấy hoặc các thông tin, tài liệu về mặt bản chất hoặc bối cảnh phải được xem / hiểu là thông tin Nội bộ thì việc chia sẻ các thông tin này phải được sự cho phép của cấp quản lý có thẩm quyền.

  INTERNAL USE ONLY: *This classification level applies to information that is strictly for use within the Company, its subsidiaries, affiliated companies, partners, or third parties, and is managed and utilized by a designated individual or group. Unauthorized disclosure of this information could violate laws, regulations, agreements with partners or third parties, and could seriously harm the Company, its customers, or its partners and third parties, including changing the company's business goals and damaging its reputation. Internal information includes but is not limited to internal and independent audit reports, security assessments, compliance evaluations, assurance reports, internal documents, employee information (salaries, bonuses, etc.), internal communication information (Personal Identifiable Information of employees for internal contact purposes), and details on models, structures, and technologies currently in use by the company. All printed or handwritten materials displaying such internal information must be stamped or labeled "NỘI BỘ" / "INTERNAL USE ONLY" on the upper/lower left/right corner of the page. Any information or documents inherently or contextually deemed internal must be treated as such, and sharing of this information must be authorized by the appropriate management level.*
- **KHÔNG PHÂN LOẠI:** là thông tin được phê chuẩn để công khai bao gồm nhưng không giới hạn như thông tin quảng bá, thông tin hỗ trợ sản phẩm, thông tin liên hệ công khai, thông tin

tuyển dụng đã được chấp nhận công khai, việc tiết lộ không gây ảnh hưởng nguy hại cho Công ty, nhân viên, các cổ đông, các Đối tác, hoặc khách hàng của Công ty.

UNCLASSIFIED: This level pertains to information that has been approved for public disclosure, including but not limited to marketing materials, product support information, public contact information, and publicly approved recruitment information. Disclosure of this information does not adversely affect the Company, its employees, shareholders, partners, or customers.

- Tất cả các thông tin Mật hay thông tin Nội bộ, bất kể vật trung gian mang thông tin (giấy, băng từ, đĩa từ, đĩa CD, thiết bị ngoại vi hoặc ổ cứng,…), bất kể hình thức thể hiện (ký tự, ảnh, video, giọng nói…), đều phải được bảo vệ chống truy cập bất hợp pháp bất cứ lúc nào.

  All Confidential, and Internal information, regardless of the medium carrying the information (paper, tape, diskette, CD-ROM, peripheral device or hard drive, etc.), regardless of the form of expression (characters, images, videos, voice, etc.) must be protected against unauthorized access at all times.

2. **Phân loại mức độ quan trọng của các ứng dụng, hệ thống / *Classification of application and system importance:***

- Tất cả các ứng dụng máy tính dùng trong hoạt động kinh doanh phải được phân loại mức độ quan trọng theo các mức độ riêng biệt: Rất Cao, Cao, Trung bình và Không phân loại. Hệ thống phân loại mức độ quan trọng này phải được sử dụng cho toàn bộ các hệ thống, ứng dụng tại Công ty, hệ thống phân loại này là một phần không thể thiếu của kế hoạch khắc phục sự cố/thảm họa. Hệ thống phân loại này cũng được dùng để xác định một sự kiện có nên đưa vào hay không trong kế hoạch khắc phục sự cố/thảm họa. Các mức độ được định nghĩa như sau:

  All computer applications used in business must be classified according to different levels of importance: Very High, High, Medium and Unclassified. This classification system must be used for all Company applications and systems as it is an integral part of the incident/disaster recovery plan. This classification system is also used to determine whether an event should be included in the incident/disaster recovery plan. The defined levels are as follows:

  - **RẤT CAO:** cấp độ này áp dụng cho các hệ thống, ứng dụng có ảnh hưởng trực tiếp tới trải nghiệm khách hàng của Công ty. Đồng thời các hệ thống, ứng dụng này trực tiếp liên quan đến quá trình sản xuất, phân phối sản phẩm, quản lý chuỗi cung ứng, quản lý hàng tồn kho, quản lý vận chuyển sản phẩm và thương mại điện tử, đòi hỏi tính sẵn sàng cao. Downtime hệ thống sẽ ảnh hưởng nghiêm trọng tới các hoạt động kinh doanh của Công ty. Do đó các hệ thống này yêu cầu:
  - *VERY HIGH: this level applies to application systems that directly impact Company's customer experience. These systems are directly related to production processes, supply chain management, inventory management, product transportation and e-commerce and require high availability. Downtime of these systems will seriously affect Company's business operations. Therefore, these systems require:*
    - **Trung tâm chính:** dữ liệu hệ thống lõi chạy mô hình clustering, dữ liệu các hệ thống khác chạy mô hình active/standby và được đồng bộ đồng thời tại Trung tâm chính. Ứng dụng chạy mô hình active/standby và được đồng bộ đồng thời tại Trung tâm chính. *Main DC: Core system data runs on a clustering model, while data from other systems runs on an active/standby model and is synchronized in real-time at the Main DC. Applications run on an active/standby model and are synchronized in real-time at the Main DC.*

- **Trung tâm dự phòng:** dữ liệu phải đồng bộ đồng thời tại Trung tâm dự phòng theo mô hình active/standby. Ứng dụng tại Trung tâm dự phòng phải giống Trung tâm chính, mỗi lần có thay đổi từ Trung tâm chính, ứng dụng phải được đồng bộ ngay sang Trung tâm dự phòng.
  DR site: data must be synchronized in real-time at the DR site using an active/standby model. Applications at the DR site must mirror the Main DC, and any changes from the Main DC must be immediately synchronized to the DR site.
- **Thời gian khắc phục sự cố:** không quá tối đa 1h làm việc kể từ khi tiếp nhận sự cố. *Incident resolution time: Maximum of 1 working hour from the time the incident is received.*

- **CAO:** cấp độ này áp dụng cho các hệ thống ứng dụng có ảnh hưởng một phần tới trải nghiệm khách hàng của Công ty hoặc các hệ thống ứng dụng hỗ trợ quản lý tài nguyên nhân sự, quản lý tài chính và kế toán cho phòng ban sản xuất và bán lẻ và các hệ thống quản lý chất lượng sản phẩm và quy trình sản xuất. Downtime hệ thống sẽ ảnh hưởng một phần tới các hoạt động kinh doanh của Công ty. Do đó các hệ thống này yêu cầu:

  HIGH: this level applies to application systems that partially impact Company's customer experience or application systems that support human resource management, financial management and accounting for production and retail departments, as well as product quality management and production processes. Downtime of these systems will partially affect Company's business operations. Therefore, these systems require:

  - **Trung tâm chính:** dữ liệu đồng bộ tần suất 1h tại Trung tâm chính theo mô hình active/standby. Ứng dụng sao lưu tại chỗ ở Trung tâm chính.
    Main DC: data must be synchronized every 1 hour at the Main DC using an active/standby model. Applications are backed up on-site at the Main DC.
  - **Trung tâm dự phòng:** dữ liệu đồng bộ tần suất 1h tại Trung tâm dự phòng theo mô hình active/standby. Ứng dụng tại Trung tâm dự phòng phải giống Trung tâm chính, mỗi lần có thay đổi từ Trung tâm chính, ứng dụng phải được đồng bộ sang Trung tâm dự phòng theo tần suất hàng ngày.
    DR site: data must be synchronized every 1 hour at the DR site using an active/standby model. Applications at the DR site must mirror the Main DC, and any changes from the Main DC must be synchronized to the DR site on a daily basis.
  - **Thời gian khắc phục sự cố:** trong khoảng từ 2h-4h làm việc kể từ khi tiếp nhận sự cố. *Incident resolution time: Within 2-4 working hours from the time the incident is received.*

- **TRUNG BÌNH:** cấp độ này áp dụng cho các hệ thống ứng dụng có ít ảnh hưởng hoặc không ảnh hưởng trực tiếp tới các khách hàng của Công ty. Downtime hệ thống ít ảnh hưởng tới các hoạt động kinh doanh của Công ty. Do đó các hệ thống này yêu cầu:

  MEDIUM: This level applies to application systems that have little or no direct impact on Company's customers. Downtime of these systems has minimal impact on Company's business operations. Therefore, these systems require:

  - **Trung tâm chính:** dữ liệu và ứng dụng được sao lưu với tần suất 8h tại Trung tâm Chính. *Main DC: Data and applications are backed up every 8 hours at the Main DC.*
  - **Trung tâm dự phòng:** dữ liệu được sao lưu sang Trung tâm dự phòng với tần suất hàng ngày.
    DR Site: data is backed up to the DR site on a daily basis.

- ➢ **Thời gian khắc phục sự cố:** trong khoảng từ 4h-8h làm việc kể từ khi tiếp nhận sự cố. *Troubleshooting time: within 4-8 working hours from the time the issue is received.*

o **KHÔNG PHÂN LOẠI:** cấp độ này áp dụng cho các hệ thống ứng dụng nội bộ không ảnh hưởng tới các khách hàng của Công ty. Downtime hệ thống không ảnh hưởng tới các hoạt động kinh doanh của Công ty. Do đó các hệ thống này yêu cầu:

This level applies to Internal application systems that do not impact Company customers. The downtime of these systems does not affect Company's business activities. These systems therefore require:

- ➢ **Trung tâm chính:** không sao lưu dữ liệu và ứng dụng tại Trung tâm chính. *Main DC: data and applications are not backed up at the Main DC.*
- ➢ **Trung tâm dự phòng:** dữ liệu sao lưu sang Trung tâm dự phòng với tần suất hàng tuần. *DR Site: data is backed up to the DR site on a weekly basis.*
- ➢ **Thời gian khắc phục sự cố:** trong khoảng từ 1-3 ngày làm việc kể từ khi tiếp nhận sự cố. *Troubleshooting time: within 1-3 working days from the time the issue is received.*

ĐIỀU 4 QUY ĐỊNH VỀ QUẢN LÝ TRUY CẬP

ARTICLE 4 ACCESS MANAGEMENT POLICY

1. Truy cập mạng nội bộ và dịch vụ mạng nội bộ / *Internal network access and internal network services*

- Bộ phận IT thực hiện quản lý truy cập mạng và các dịch vụ mạng nội bộ theo quy định tại Quy định về Yêu cầu & Quản lý ACL.

  IT Departments are responsible for managing network access and internal network services according to the regulations in the Requirements & ACL rules Management Policy.

- Thực hiện các biện pháp kiểm soát chặt chẽ các kết nối từ mạng không tin cậy vào mạng nội bộ của Công ty.

  Implement strict control measures for connections from untrusted networks to Company's internal network.

- Kiểm soát việc cài đặt, sử dụng các công cụ phần mềm hỗ trợ truy cập từ xa. Nếu cung cấp các phương thức xác thực để nhân viên truy cập mạng nội bộ thì cần phải đảm bảo các điều kiện sau:

  Control the installation and use of remote access support tools. If authentication methods are provided for employees to access the internal network, the following conditions must be ensured:

  - Các phương thức xác thực này nếu đã cấp cho một tài khoản cá nhân thì không được chia sẻ cho các tài khoản khác.

    These authentication methods, if granted to an individual account, must not be shared with other accounts.

  - Kết nối từ mạng Internet vào mạng nội bộ của Công ty để phục vụ công việc phải sử dụng mạng riêng ảo (VPN) và xác thực đa nhân tố.

    Connections from the Internet to Company's internal network for work purposes must use a virtual private network and multi-factor authentication.

2. Quản trị tài khoản và quyền / *Account and privilege management*

- Người dùng nội bộ và bên ngoài Công ty phải được định danh (ID) duy nhất và chứng thực rõ ràng trước khi được cấp quyền truy cập hệ thống;

Internal and external users of Company must have a unique identification (ID) and clear authentication before being granted system access;

- Định danh (ID) đã hết hạn (expired) hoặc bị hủy kích hoạt (deactivated) sẽ không được cấp lại cho cá nhân khác;

  Expired or deactivated IDs will not be reissued to other individuals;

- Hành động cấp quyền, chỉnh sửa, thu hồi quyền phải nhận được sự phê duyệt từ cấp quản lý thích hợp;

  Authorization, modification or revocation actions must receive approval from the appropriate management level;

- Tài khoản, quyền của người dùng đã nghỉ / chuyển việc phải được thu hồi ngay;

  Accounts and privileges of users who have left /changed jobs must be revoked immediately;

- Định kỳ 6 tháng rà soát tài khoản và quyền của người dùng;

  User accounts and privileges must be reviewed every 6 months;

- Đảm bảo tài khoản / quyền hạn không còn hợp phép phải được xóa khỏi hệ thống;

  Ensure that unauthorized accounts / privileges are deleted from the system;

- Kết nối từ phân vùng người dùng đến hệ thống CNTT quan trọng phải thông qua máy chủ quản trị (terminal access) và phải xác thực đa nhân tố. Terminal access phải được đặt trong vùng mạng quản trị, không được phép truy cập Internet, được cài đặt ứng dụng chống phần mềm/mã độc hại và chỉ cài tối thiểu các phần mềm cần thiết dành cho việc quản trị.

  Connections from user partitions to critical IT systems must go through an administrative server (terminal access) and must have multi-factor authentication. Terminal access must be placed in the administrative network zone, not allowed to access the Internet, installed with anti-malware / malicious code applications, and only minimal necessary software for administration purposes.

- Các tài khoản đặc quyền không định danh mặc định (root, administrator, v.v.) phải được vô hiệu hóa đăng nhập (ngay cả trong tình huống truy cập từ xa). Người dùng quản trị chỉ được phép sử dụng sudo (unix), run as (Windows) trên hệ điều hành quản trị.

  Default privileged accounts (root, administrator, etc.) must be disabled for login (even in remote access situations). Administrative users are only allowed to use sudo (unix), runas (Windows) on the administrative operating system.

- Tên tài khoản đặc quyền phải được đặt sao cho có thể xác định người sử dụng và mỗi người quản trị phải chịu trách nhiệm về tài khoản của mình.

  Privileged account names must be set in a way that identifies the user, and each administrator is responsible for their own account.

3. Mật khẩu / *Passwords*

- Người dùng có trách nhiệm bảo vệ Mật khẩu của mình.

  Users are responsible for protecting their passwords.

- Không được chia sẻ bí mật chứng thực cho bất kỳ ai. Bí mật chứng thực được xem như là thông tin Mật của Công ty.

  Do not share authentication secrets with anyone. Authentication secrets are considered Company's Confidential information.

- Không truyền Mật khẩu (dạng clear text—không có mã hóa) qua email, sử dụng kênh trao đổi khác để thông báo Mật khẩu, hoặc chỉ gửi link kích hoạt qua email để tạo / tái tạo Mật khẩu lần đầu.

  Do not transmit passwords (in clear text—unencrypted form) via email, use other channels for password notification, or only send activation links via email to create / reset passwords for the first time.

- Mật khẩu phải luôn được mã hóa trong quá trình truyền thông trên hệ thống, không được hiển thị ở bất kỳ dạng văn bản có thể đọc được.

  Passwords must always be encrypted during transmission on the system and must not be displayed in any readable text form.

- Độ dài của Mật khẩu ít nhất là 08 ký tự phải gồm tổ hợp các ký tự: chữ hoa, chữ thường, số và ký tự đặc biệt (!@#$%^&*(),...).

  The password length must be at least 08 characters and must consist of a combination of uppercase letters, lowercase letters, numbers, and special characters (!@#$%^&(),...).*

- Khi đăng nhập sai 05 lần tài khoản sẽ bị tạm thời khóa lại trong 30 phút và chỉ có quản trị viên hệ thống mới có thể mở lại tài khoản này.

  When logging in incorrectly 05 times, the account will be temporarily locked for 30 minutes and only the System Administrator can unlock this account.

- Mật khẩu phải được thay đổi sau 180 ngày.

  Password must be changed after 180 days.

- Mật khẩu cung cấp lần đầu cho người dùng phải là duy nhất và yêu cầu thay đổi ngay sau lần sử dụng đầu tiên.

  The initial password provided to users must be unique and require immediate change after the first use.

- Bộ phận IT của Công ty phải kiểm soát lại quy trình đăng nhập và các thao tác đăng nhập thành công và không thành công cũng như các quá trình thay đổi Mật khẩu. Cần phải ghi lại các thao tác của tài khoản đặc quyền trong suốt quá trình truy cập.

  The login process and successful / unsuccessful login attempts, as well as Password changes, must be monitored by IT Department. All actions of privileged accounts must be recorded throughout the access process.

- Mọi nghi ngờ về lộ Mật khẩu phải báo ngay cho Bộ phận ISO / IT và thực hiện thay đổi toàn bộ Mật khẩu đang dùng.

  Any suspicion of password leakage must be immediately reported to the IT / ISO Department and all Passwords in use must be changed.

ĐIỀU 5 XỬ LÝ KỶ LUẬT AN TOÀN THÔNG TIN

ARTICLE 6 INFORMATION SECURITY DISCIPLINARY ACTIONS

Tùy theo mức độ vi phạm Quy định này và/hoặc Quy định nội bộ liên quan khác, người vi phạm bị xử lý theo các hình thức sau:

Depending on the severity of the violation of this Policies and/or other relevant Internal Regulations, the offender will be subjected to the following disciplinary measures:

- Khiển trách bằng miệng/email: vi phạm lần đầu hoặc không thực hiện các yêu cầu trong quy định về an toàn thông tin mà không có lý do chính đáng và không gây hậu quả nghiêm trọng;

Oral/email reprimand: for first-time violations or for not complying with information security regulations without a valid reason and without causing serious consequences;

- Khiển trách bằng văn bản: vi phạm lần thứ hai và không gây hậu quả nghiêm trọng;

  Written reprimand: for a second violation that also did not result in serious consequences;

- Hình thức "kéo dài thời gian nâng lương" hoặc "cách chức": có hành vi phá hủy dữ liệu Công ty hoặc không tuân thủ Quy định nội bộ hoặc không thực hiện các biện pháp an ninh thông tin hoặc không ứng phó kịp với những sự cố an ninh, dẫn đến thiệt hại, hậu quả cho Công ty.

  "Delay in salary increase" or "demotion": for destroying Company data or not adhering to Internal Regulations or failing to implement information security measures or not responding promptly to security incidents, resulting in Company consequences / damage.

- Hình thức sa thải: có hành vi cố ý gây hậu quả nghiêm trọng về bảo mật thông tin hoặc không tuân thủ Quy định nội bộ, dẫn đến thiệt hại tài sản, uy tín, lợi ích nghiêm trọng của Công ty.

  Dismissal: for intentionally causing serious consequences regarding information security, failing to follow Internal Regulations resulting in serious damage to Company assets/interests/prestige.

- Nhân viên vi phạm Quy định này và/hoặc Quy định nội bộ liên quan ngoài việc phải bồi thường cho Công ty, còn có thể bị truy tố trách nhiệm hình sự.

  Employees who violate this Policy and/or Internal Regulations must compensate the Company and may also face criminal prosecution.