



✉ 8th floor, 18/11 Thai Ha, Hanoi
✉ vietnam@exoplatform.com
✉ +84 4 628 50000
✉ www.exoplatform.com

IT RESOURCES USAGE POLICY QUY ĐỊNH SỬ DỤNG TÀI NGUYÊN CNTT

1. PURPOSE/ MỤC ĐÍCH

The purpose of this policy is to regulate how to use computers, equipment and internal networks safely, efficiently; Make employees work in best possible conditions; Tell how to protect assets (physical, intangible) that eXo Platform SEA owns and uses, in order to reduce amount of threat from inside and outside the company.

Mục đích của Quy Định này là nhằm quy định cách thức sử dụng máy tính, thiết bị và mạng nội bộ an toàn, hiệu quả; Giúp nhân viên làm việc trong các điều kiện tốt nhất; Đưa ra cách thức bảo vệ các tài sản (hữu hình và vô hình) do Công ty eXo Platform SEA sở hữu và sử dụng để giảm thiểu các mối đe dọa cho công ty và toàn thể nhân viên từ cả các tác nhân bên trong và bên ngoài.

2. SCOPE/ PHẠM VI

This policy applies to all users of eXo Platform SEA systems and networks. In the following text, "company" refers to eXo Platform SEA; "user" refers to anyone who accesses a company network, service or equipment; "equipment" refers to any digital device operated by the user; "document" refers to the IT Resources Usage Policy you are presently reading.

Quy Định này áp dụng cho tất cả các người sử dụng trong cơ sở hạ tầng hệ thống và mạng của eXo Platform SEA. Trong văn bản sau, "công ty" là để chỉ công ty eXo Platform SEA; "người dùng" là để chỉ người truy cập mạng, dịch vụ hoặc thiết bị của công ty; "thiết bị" là để chỉ tất cả các thiết bị kỹ thuật số được sử dụng và vận hành bởi người dùng; "văn bản" là để chỉ Quy Định Sử Dụng Tài Nguyên CNTT.

S.G.C.

3. CONTENT/ NỘI DUNG

3.1. Equipment Usage Policy/ Quy Định Sử Dụng Thiết Bị

3.1.1. Hardware Usage Policy/ Quy Định Sử Dụng Phần Cứng

- The user is responsible for safe preservation of equipment provided and commits to compensate for any loss or damage if his or her liability is involved.
Người dùng phải có trách nhiệm bảo quản các trang thiết bị được cấp phát và cam kết bồi thường trong trường hợp mất mát hay hư hỏng do người dùng gây nên.
- The user must explain reasons and specify responsibilities clearly for any encountered loss or damage.
Người dùng phải giải trình rõ nguyên nhân và qui trách nhiệm rõ ràng về mọi hư hỏng hoặc mất mát khi gặp phải.
- Equipment used at home must be managed appropriately and securely. It must be used for company purpose only. The company has the right to remove the permission for bringing equipment home in any circumstance. If the user is authorized to bring equipment at home, his or her responsibilities are defined in an official authorization document.
Các thiết bị được mang về nhà phải được bảo quản cẩn thận và an toàn và chỉ được sử dụng cho mục đích công việc. Công ty có quyền tước quyền mang laptop về nhà, nếu người dùng không tuân theo một trong các quy định trong văn bản này. Nếu người dùng được phép mang thiết bị về nhà, trách nhiệm khi sử dụng thiết bị của người dùng đồng thời cũng được nêu rõ trong Biên Bản Cho Phép Mang Thiết Bị Ra Khỏi Công Ty.
- The user must not open the machine cover or remove screws, latches of the machine cover.
Người dùng không được tự ý mở nắp máy, tháo bỏ các vít, chốt của vỏ máy.
- The user must not remove and tear off the company labels or warranty stamps on equipment or components.
Người dùng không được bóc và làm rách các tem của công ty hoặc tem bảo hành đã dán lên từng thiết bị hoặc linh kiện.

- The user must not make any addition or alteration to the equipment without the consent of the company.
Người dùng không được tự ý lắp thêm hoặc gỡ bỏ linh kiện hay thiết bị bên trong máy mà không có sự cho phép của công ty.
 - The user must not sabotage components and equipment of any kind.
Người dùng không được phá hoại các linh kiện, thiết bị dưới bất kỳ hình thức nào.
- Caution/ Lưu ý:
- After submitting a resignation, the user is no longer allowed to bring company devices at home
Sau khi nộp đơn xin thôi việc, người dùng không được phép mang các thiết bị công ty cắp phát về nhà.
 - To guarantee security of internal network, the user must not bring personal equipment to the company and access company network or company equipment of any kind (the following list of examples is by no means exhaustive: wired network, WiFi network, sharing network via company equipment).
Để đảm bảo an toàn của mạng nội bộ công ty, người dùng tuyệt đối không được mang thiết bị cá nhân và truy cập vào mạng hoặc thiết bị của công ty dưới bất kỳ hình thức nào (Danh sách sau có thể chưa liệt kê được đầy đủ tất cả các trường hợp: mạng có dây, mạng không dây, chia sẻ mạng thông qua thiết bị công ty và một số hình thức khác).
 - Team Leaders are responsible to ensure that usage of equipment inside their team complies with the current document.
Các Team Leader có trách nhiệm đảm bảo sự sử dụng của các thiết bị trong team tuân theo đúng Quy Định Sử Dụng Tài Nguyên CNTT hiện thời.

3.1.2. Software Usage Policy/ Quy Định Sử Dụng Phần Mềm

- The user must not add different software from that listed in the document made when equipment is assigned to him or her.
Người dùng không được cài đặt bất kỳ phần mềm nào nằm ngoài danh sách công ty cung cấp cho người dùng.
- The user is legally fully responsible for the installation of all additional software found on his or her machine but not given in that list.
Người dùng phải hoàn toàn chịu trách nhiệm pháp lý cho việc phát hiện những phần mềm được cài trên máy của người dùng mà không nằm trong danh sách của công ty.
- The user must not remove any software installed by the company. If the work requires any change on the equipment configuration or installed software, he or she must first discuss with the company and get its approbation.
Người dùng không được tự ý gỡ bỏ các phần mềm đã được cài bởi công ty. Nếu công việc yêu cầu bất kỳ thay đổi nào trong cấu hình thiết bị hoặc phần mềm đã được cài đặt, người dùng phải trước hết thảo luận với công ty và phải có được sự đồng thuận.
- The user must not copy or distribute any software which license was bought by the company or for which the company obtained a usage authorization.
Người dùng không được sao chép hoặc lưu truyền bất kỳ phần mềm có bản quyền nào đã được công ty mua hoặc công ty có quyền sử dụng hợp pháp.
- If the user's equipment was equipped with antivirus application, then the user must keep it enabled.
Alerts about infected viruses must be reported to the company.
Nếu máy tính của người dùng được cài đặt phần mềm phòng chống virus, người dùng phải luôn đặt nó trong trạng thái kích hoạt bảo vệ. Tất cả thông báo về các virus đã lây nhiễm phải được báo cáo cho công ty.
- The user must notify the company if mistakes in software usage are detected.
Người dùng phải có trách nhiệm thông báo những sai phạm về sử dụng phần mềm khi phát hiện được cho công ty.



3.1.3. Account Usage Policy/ Quy Định Sử Dụng Tài Khoản

- The user is responsible for any account he or she has been given.
Người dùng phải chịu trách nhiệm cho mỗi tài khoản được cấp phát của mình.
- The user must change password when receiving an account from the company. The password should not be easily guessed and match following standards:
Người dùng phải thay đổi mật khẩu sau khi được cấp bởi công ty. Mật khẩu không nên dễ đoán và đảm bảo được các tiêu chuẩn sau:
 - Password should have at least 6 characters.
Nên có tối thiểu 6 ký tự.
 - Password should have a certain complexity. The following types of characters must at least be represented once :
Nên có tính phức hợp. Các kiểu ký tự sau phải ít nhất hiện diện một lần:

- Uppercase (A...Z)
Chữ hoa (Từ A...Z)
- Lowercase (a...z)
Chữ thường (Từ a...z)
- Digit (0...9)
Số (Từ 0...9)

- The user should change his or her password regularly, every 90 days.
Người dùng nên thay đổi mật khẩu thường xuyên 90 ngày một lần.
- The user must keep his or her password secret. The user must not share or reveal his or her password to anyone.
Người dùng phải giữ mật khẩu an toàn. Người dùng không được chia sẻ hoặc để lộ mật khẩu cho bất kỳ ai.
- The user must also not use an account not belonging to him or her. If the user discovers that someone made an unauthorized use of his or her account, he or she must immediately change his or her password and report the issue to the company.
Người dùng cũng không được sử dụng tài khoản không thuộc của mình. Nếu phát hiện ra người khác đã sử dụng bất hợp pháp tài khoản của mình, người dùng phải lập tức thay đổi mật khẩu và đồng thời phải nhanh chóng thông báo cho công ty.

3.1.4. Computer Operation Policy/ Quy Định Vận Hành Máy Tính

- The user must not change password configuration such as (the following list is by no means exhaustive) BIOS Setup password, HDD password... to the equipment without the authorization of the company.
Người dùng không được thay đổi các loại mật khẩu trong cấu hình hệ thống như (Danh sách sau có thể chưa liệt kê được đầy đủ tất cả các trường hợp) mật khẩu thiết lập BIOS, mật khẩu cho ổ đĩa cứng... cho thiết bị mà không được sự cho phép của công ty.
- The user must use the equipment for tasks related to the work of the company only.
Người dùng phải sử dụng máy tính cho mục đích công việc.
- The user must set a password for the account used in the computer.
Người dùng phải đặt mật khẩu cho tài khoản sử dụng trên máy tính.
- The user must lock the screen when he or she is away from the equipment.
Người dùng phải thực hiện thao tác khóa màn hình khi rời khỏi thiết bị.
- The user must immediately inform the company when the equipment has abnormal symptoms or if any incident happened to it, in order to allow a timely recovery.
Người dùng phải báo ngay cho công ty khi có hiện tượng bất thường hoặc sự cố máy tính để kịp thời khắc phục.
- If not needed, the user should not bring equipment to attend meetings, presentations or trainings. This is to allow a maximum focus and avoid disturbing others.
Nếu không cần thiết, người dùng không nên mang máy tính vào tham dự các buổi thuyết trình, các buổi họp, các buổi đào tạo. Điều này cho phép tập trung tối đa và tránh làm phiền những người khác.
- Before leaving the office, the user must shut down the computer safely and wait for the completion of the shutdown.
Trước khi rời khỏi công ty, người dùng phải tắt máy tính và đợi đến khi máy tắt hẳn mới rời khỏi chỗ làm việc.
- The user must not use the computer of another user without the approval of the company.
Người dùng không được sử dụng máy tính của người dùng khác mà chưa được sự cho phép của công ty.

430
;ON
CH NH
TO PLA
VG E

3.2. Email Usage Policy/ Quy Định Sử Dụng Email

- The user must not send through company email messages including bad content (the following list is by no means exhaustive): pornographic, terrorism, extortion.... The user must not send emails against the interests of the company.
Người dùng không được gửi các email bao gồm những nội dung sau (Danh sách sau có thể chưa liệt kê được đầy đủ tất cả các trường hợp): khiêu dâm, khủng bố, tống tiền... Người dùng không được gửi các email chống phá các lợi ích của công ty.
- The user must not forward information belonging to the company to recipients outside the company without the prior authorization from the company.
Người dùng không được chuyển tiếp các thông tin thuộc về công ty đến những người bên ngoài mà không được sự cho phép ưu tiên từ phía công ty.
- The user must not hide sender's email address.
Người dùng không được sử dụng bất kỳ thủ thuật nào để che dấu địa chỉ người gửi.
- The user must not open emails that are reported as suspicious by email software advisor. He or she

must ask advice from the company before.

Người dùng không được mở các email mà bộ lọc email đã thông báo là có khả năng nguy hiểm. Người dùng phải hỏi ý kiến công ty trước.

- The user must not open attachments in emails sent from strange, suspicious or hidden email addresses.

Người dùng không được mở các file đính kèm trong các email được gửi từ những người lạ, có nghi ngờ hoặc các email ẩn danh.

- The user should set email filtering rules to separate clearly between work and private emails.

Người dùng nên thiết lập các luật lọc email để phân biệt rõ ràng các email công việc và email cá nhân.

- The user should enable spam filtering feature to avoid being impacted by junk emails.

Người dùng phải kích hoạt chức năng lọc email rác để tránh bị ảnh hưởng bởi các email xấu hoặc email quảng cáo.

- If the user has any complain, suggestion or question related to policy/benefit/plans of the company, he or she must send an email to the related person. He or she must not send such emails to mailing lists or all users, to avoid disturbing all staff.

Khi có bất kỳ thắc mắc, phản nản hoặc câu hỏi gì về các vấn đề liên quan đến công ty như chính sách, lợi ích hoặc kế hoạch, người dùng phải gửi email đến người liên quan, phụ trách về vấn đề đó. Người dùng không được gửi các email như trên đến các mailing list hoặc cho tất cả người dùng trong công ty, nhằm tránh tình trạng làm ảnh hưởng đến tất cả các nhân viên khác.

- The user must not send emails with inappropriate content such as complains, worries, thoughts, gossips, crap stories, rumors or topics not directly related to work to company mailing lists or all users.

Người dùng không được gửi các email với nội dung không thích hợp như phản nản, lo lắng, cảm nghĩ, truyện tắm phao, truyện tục, tin đồn hoặc các chủ đề không liên quan đến công việc vào các mailing list của công ty hoặc cho tất cả người dùng khác trong công ty.

- The user must leverage company mailing lists only if the content of his or her email matches the interest of the recipients.

Người dùng chỉ được sử dụng các mailing list nếu nội dung email thích hợp với sự quan tâm của người nhận.

- The user must not send emails on behalf of others in company without the consent of him or her.

Người dùng không được nhân danh người khác trong công ty gửi email mà không được sự đồng ý và cho phép của người đó.

- The user must not intercept, sniff, hijack or change content of emails sent in the company.

Người dùng tuyệt đối không được chặn, bắt, nghe trộm và thay đổi nội dung của các email được gửi trong công ty.

- The user must not use alternate email services such as (the following list is by no means exhaustive) Yahoo Mail, Gmail, Hotmail... to convey company emails or data.

Người dùng không được sử dụng các dịch vụ email thay thế khác như (Danh sách sau có thể chưa liệt kê được đầy đủ tất cả các trường hợp) Yahoo Mail, Gmail, Hotmail... để chuyển các email hoặc dữ liệu của công ty.

- The user must not use company emails to register to bad or blocked websites.

Người dùng không được sử dụng email của công ty đăng ký làm thành viên của các trang web xấu hoặc bị cấm.

1045
G T
M H
FORN

X-1

3.4. Company Data Usage Policy/ Quy Định Sử Dụng Dữ Liệu Công Ty

- The user must not send private company data to anyone who does not belong to the company without prior approval from the company. This includes any information exchange medium (The following list of medium is by no means exhaustive: instant message services, software, email...).

Người dùng không được gửi dữ liệu công ty cho bất kỳ ai bên ngoài công ty mà không có sự cho phép của công ty. Điều này bao gồm bất kỳ một môi trường trao đổi thông tin nào (Danh sách sau có thể chưa liệt kê được đầy đủ tất cả các trường hợp: các phần mềm chat, email...)

- The user is directly responsible for securing the company data on private storages (the following list of storages is by no means exhaustive: USB stick, external HDD, optical disc, mobile) to reduce risk of data loss or interception by other parties. The user is strongly encouraged to encrypt data.

Người dùng có trách nhiệm bảo đảm an toàn dữ liệu công ty trên các thiết bị lưu trữ cá nhân (Danh sách sau có thể chưa liệt kê được đầy đủ tất cả các trường hợp: USB, ổ cứng di động, đĩa quang, mobile) để giảm thiểu sự mất mát dữ liệu hoặc sự can thiệp bởi các bên khác. Người dùng được khuyến khích mã hóa dữ liệu.

- The user must not upload private data or data not related to work on local storage.

Người dùng không được upload các dữ liệu cá nhân hoặc dữ liệu không liên quan đến công việc lên storage nội bộ.

- The user must not intentionally corrupt or destroy data of other users or teams in local storage.

Người dùng không được cố ý phá hủy hoặc làm hỏng dữ liệu của team hoặc của người dùng khác trên storage nội bộ.

3.3. Network Usage Policy/ Quy Định Sử Dụng Mạng

- The user must not access internet during working time for following purposes:
Người dùng không được truy cập Internet trong giờ làm việc vào các mục đích sau:
 - Sharing or downloading files using peer-to-peer software (the following lists is by no means exhaustive: Kazza, emule, dropbox, torrent...)
Chia sẻ hoặc tải về các file bằng cách sử dụng phần mềm chia sẻ ngang hàng (Danh sách sau có thể chưa liệt kê được đầy đủ tất cả các trường hợp: Kazza, emule, dropbox, torrent...)
 - Receiving online streams (the following list is by no means exhaustive: music, radio, movies...)
Sử dụng các dịch vụ online giải trí (Danh sách sau có thể chưa liệt kê được đầy đủ tất cả các trường hợp: nhạc, radio, phim...)
 - Playing online game
Chơi game trực tuyến
 - Downloading games or other entertainment software
Download các trò chơi hay các phần mềm giải trí khác
 - Reading digital news, papers not related to work
Xem báo, tin tức điện tử mà không liên quan đến công việc
 - Accessing content that relate to entertainment
Truy cập các nội dung liên quan đến giải trí
 - Accessing websites, blogs, forums that not related to work
Truy cập các website, blog, diễn đàn mà không liên quan đến công việc.
- The user must not access websites that are bad, abusive and pornographic or websites that provide illegal software, hacked serial keys...
Người dùng không được truy cập vào trang web có nội dung xấu, đồi trụy, không lành mạnh và các trang web cung cấp phần mềm, serial key bất hợp pháp.
- The user must discuss with company before downloading or uploading reasonably big packages that could impact the bandwidth during working time.
Người dùng phải thảo luận với công ty trước khi muốn download hoặc upload các gói tin có dung lượng quá lớn mà có thể làm ảnh hưởng đến tốc độ đường truyền internet trong giờ làm việc.
- The user must not access websites that are reported as suspicious by web browser advisor. He or she must ask advice from the company first.
Người dùng không được truy cập vào các trang web mà trình duyệt đã báo cáo là có khả năng nguy hiểm hoặc giả mạo. Người dùng phải hỏi ý kiến công ty trước.
- The user must not provide access to unauthorized remote locations to other users' machines.
Người dùng không được truy cập và cung cấp truy cập từ xa bất hợp pháp vào máy tính của các người dùng khác.
- The user must not install or use software or devices that have analytic or intrusive features such as (the list is by no means exhaustive): interrupting, sniffing, hijacking or eavesdropping in company network.
Người dùng không được cài đặt hoặc sử dụng phần mềm hoặc thiết bị có chức năng phân tích hoặc xâm nhập như (Danh sách sau có thể chưa liệt kê được đầy đủ tất cả các trường hợp): ngăn chặn, thăm dò, bắt hoặc nghe trộm trong mạng công ty.
- The user must not study or use procedures to investigate servers or equipment of the company.
Người dùng không được nghiên cứu hoặc sử dụng bất kỳ thủ thuật nào để tìm hiểu các server, thiết bị của công ty.
- The user must not attempt to illegally access to company servers or equipment.
Người dùng không được tìm cách truy cập bất hợp pháp vào các máy chủ hoặc thiết bị nằm trong mạng công ty.
- The user must not attempt to attack any company service.
Người dùng không được tìm cách tấn công vào bất kỳ một dịch vụ nào do công ty quản lý.
- The user must not attempt to attack any outside server, website or equipment from company network.
Người dùng không được tìm cách tấn công vào bất kỳ server hoặc website nào bên ngoài mạng của công ty.
- The user must not use software or device for purpose to bypass company proxy or firewall.
Người dùng không được sử dụng phần mềm hoặc thiết bị nhằm mục đích vượt qua proxy hoặc tường lửa của công ty.
- In the course of using local network and internet, the user must notify the company immediately if he or she detects violations or prohibited actions.
Trong quá trình sử dụng mạng nội bộ và internet người dùng phải thông báo ngay cho công ty nếu phát hiện những trường hợp vi phạm các hành vi bị cấm.



Caution/ Lưu ý:

- In order to guarantee the security of the network and of the machines, the user must not access non official eXo networks. This notably includes (the following list is by no means exhaustive) other wireless networks, or 3G, 4G networks.
Để đảm bảo an toàn cho mạng và các máy tính, thiết bị của công ty, người dùng tuyệt đối không được truy cập vào các mạng bên ngoài eXo. Trong đó bao gồm (Danh sách sau có thể chưa liệt kê được đầy đủ tất cả các trường hợp): các mạng không dây khác hoặc các mạng 3G, 4G...
- In emergency case (network or internet failure), if the user wishes to access to other network (eg: WiFi or 3G), he or she must request a prior authorization from the company.
Trong trường hợp khẩn cấp (lỗi mạng hoặc internet) nếu người dùng muốn truy cập mạng khác (VD: WiFi hoặc 3G), người dùng phải có sự cho phép ưu tiên từ phía công ty.


Tran Nguyen Son Tung
P.Quản Trị HT và Mạng
IT Manager


Nguyen Viet Long
P.Hành Chính
Office Manager


CÔNG TY
TRÁCH NHIỆM HỮU HẠN
EXO PLATFORM SERVICES VIETNAM
ĐỒNG HÀNH


Brice Claude Révenant
Giám Đốc
General Manager


N.NG 1/04