2021

Internet & Email Policy for HECNY GROUP

STAFF SHALL READ THIS POLICY AND THIS POLICY HAS BEEN PUBLISHED IN URL BELOW
http://www.hecny.com/download/ITpolicy-internetandeamil.pdf

HECNY GROUP

September 2020

Table of Contents

Introduction

HECNY GROUP aims to provide the best and useful tools to facilitate communication with business partners like oversea agents, co-loaders, vendors, and customers, as well as own brother stations, in order to allow our staffs with accessible, up-to-date and reliable information to support you in business development, daily operation and communication.

Now-a-days, achieving this goal is a big challenge in the Internet world, as especially, sending E-mail in and out and browsing internet are being part of our activities to communicate and research information for freight and logistics management, just like tracing the container status and cargo arrival to fulfill the customer satisfaction. However, we need to tackle the malicious attack in any form that happening in Internet every day to maintain our service level and make our information secure but accessible. Therefore, both tools are provided to you at a significant cost.

As a user, we must understand that this access right is for business development and daily operation purpose and not for personal activities. Users must also understand that any connection to the illegal websites, Junk mails or Ransomware offer an opportunity for non-authorized users to view or access the company information. Therefore, it is important that all connections be secure, controlled and monitored to provide a stable and reliable internet environment to support you in your daily work and electronic communication.

Communication Facility

It is supported by both computer hardware and user account maintenance; the majority will be classified as below:

1. Personal computers, e.g. PC, Notebook, Netbook
2. Mobile E-mail devices, e.g. Blackberry; IOS(Apple), Android
3. Communication Tools, e.g. SKYPE, QQ, Zoom
4. E-mail Account, i.e. has been setup in Enterprise E-mail Server(s)
5. Internet Account, i.e. has been granted to access via the Personal Computer

Stakeholders

It is applicable to all HECNY Staffs, when they are using Communication Facility to communicate with both internal and external parties for any business activity.

Staff is

1. A user who can access HECNY or subsidiary E-mail accounts
2. A user who can access Internet with the personal computer or mobile device (like Notebook, and Blackberry) for daily operation
3. A user who can connect to our Internal Network, including, network folders, and transactional databases.

Communication Tools

Communication Tools is a form of electronic communication enabling ad hoc collaboration through sending and receiving messages almost instantaneously across a network connection. This can be via mobile communication devices or via Internet connected computers. Since the introduction of popular messaging tools such as WhatsApp and WeChat, more and more people are enjoying the convenience and ease provided by real-time messaging in their day-to-day life. It is now not just a personal tool, but also a business communication channel in the workplace for customer services, such as communicating with customers and partners, offering customer support, receiving real-time alerts and project coordination.

The following tools are currently we support:

1. SKYPE – for both voice and messaging communication
2. QQ – for messaging only and using in China
3. WhatsApp
4. Line
5. WeChat
6. Zoom – for video conferencing

Please…..

- Don't set your IM client to automatically accept file transfers. If you do, you place yourself at very high risk of automatically accepting virus-infected files unknowingly.
- Don't click on URL links from un-trusted / unknown contacts in IM.
- Don't send personal or sensitive information over IM networks without encryption.
- Don't disclose contact lists used for batch submissions.
- Disable all network services provided by the IM service.
- Disable sharing of resources and disable remote activation of microphones and video cameras when using IM service.

E-mail Use

HECNY E-mail account is authorized for daily business activities purposes (including sales and business development, customer services, daily operation, documentation and exchange, where all connects to any customer enquiry, booking, shipping document submission and rate enquiry, billing and payment issue, as well as internal process communication).

Implementation of this policy ensures that staffs have access to this critical form of communication. For the majority of staffs, this will not represent any change from what is currently done; it will, however, ensure that all staffs can access, and be accessed by, E-mail as the need arises.

1. Company uses of E-mail
   E-mail is one of the official means for communication within HECNY. Therefore, the company has the right to send communications to staffs via E-mail and the right to expect that those communications will be received and read in a timely fashion.

2. Assignment of staff E-mail addresses
   HECNY's E-mail Administrator will assign staffs an official E-mail address that mentioned in the "List of Domains" section). E-mail administrator will update the Address List from time to time when the request is being sent by brother stations and Human Resources Department with management approval.

3. Redirecting and Forwarding of personal E-mail
   You are not recommended to redirect your personal E-mail communication at your personal E-mail address (e.g. @outlook.com, @hotmail.com, @yahoo.com, @gmail.com and so on) to and from HECNY's E-mail address. The Company will not be responsible for the handling of E-mail by any outside parties that are not under managed.

   You are prohibited from using third-party email systems and storage servers to conduct company business, to create or memorialize any binding transactions, or to store or retain email on behalf of company. Such communications and transactions should be conducted through proper channels using company approved documentation.

4. Appropriate use of Staff E-mail
   In general, E-mail is not appropriate for transmitting sensitive or confidential information unless its use for such purposes is matched by an appropriate level of security. For detail information, you can contact IT Department for further assistance.

Storage of E-mail messages and documents

E-mail is being part of our message exchange activity every day. As an Enterprise system infrastructure well-defined, we cannot guarantee an unlimited storage for each user within the E-mail system, because of the capacity planning and system performance concerns. Therefore, you are liable to maintain your mailbox size and keep it under a manageable and health condition that will help minimize the impact on daily E-mail system operation.

There are two ways to comply with this:

1. Create a Personal folder (.pst file) in your E-mail account in which you save these messages. Back up your files appropriately; do not delete these messages. Save the E-mail message to your PC's hard disk as a file.

2. Print out a paper copy and save it in an appropriate file if it is necessary, e.g. Cargo Claim, Accounting Audit. It is highly recommended THINK BEFORE YOU PRINT, because we need to gain the operation saving and support the environment protection for our future.

Authentication and Authorization

Company Property

- E-mail services are extended for the use of appropriately authorized users to accomplish tasks related to and consistent with the company's mission.
- Any E-mail address or account assigned by the company to individuals, subunits, or functions of the company, is the property of the company.

Authorized Service Restrictions

- E-mail users are required to comply with local law, company policies, and normal standards of professional and personal courtesy and conduct.
- Access to company E-mail services is a privilege that may be wholly or partially restricted by the company without prior notice and without the consent of the E-mail user:
  a) When required by and consistent with applicable law or policy.

  b) When there is a reasonable suspicion that violations of policy or law have occurred or may occur

c) When required to meet time-dependent, critical operational needs. Such access restrictions are subject to the approval of the appropriate company supervisory or management (i.e. Top Management, department heads, station managers.).

Authorized Access and Disclosure

- The company may permit the inspection, monitoring, or disclosure of Email in certain circumstances.
- Users are required to comply with company requests for access to and copies of company E-mail records when access or disclosure is required or allowed by applicable law or policy, regardless of whether such records reside on a computer housed or owned by the company. Failure to comply with such requests can lead to disciplinary or other legal action pursuant to applicable law or policy, including but not limited to appropriate company personnel policies or Codes of Conduct.

Misuse

- Using E-mail for illegal activities is strictly prohibited.
- Failure to follow the law with regard to the disposition of mail records can lead to criminal charges.
- Company E-mail services may not be used for personal activities not approved by the appropriate company supervisory or management.
- Applicable company policies include, but are not limited to, those policies and guidelines regarding personnel, intellectual property, or those regarding sexual or other forms of harassment.
- E-mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the company or any unit of the company unless expressly authorized to do so.

Email Signature Standard

An official HECNY email signature consists of this information:

Line 1: First and Last Name (text is red; middle initial optional; title such as “Dr.” is permitted)
Line 2: Company Name
Line 3: office: 852-XXXX-XXXX | mobile: 852-XXXX-XXXX (mobile # is optional)
Line 4: yourname@hecny.com | www.hecny.com
Line 5: Company address

Sample:
Ken William
Hecny Transportation LTD
T: +852 2751 4300   M: +852 9003 53xx
E: kenwilliam@hecny.com | www.hecny.com
A: 11/F, Hecny Centre, 111 Wai Yip Street, Kwun Tong, Hong Kong

****
****
All business transactions of our company are subjected to the Standard Trading Conditions (STC) and all ocean shipments are subjected to the Terms and Conditions of Hecny House Bill of Lading.
In the event of conflict between the terms of the STC and terms of the Hecny House Bill of Lading, the terms of the Hecny House Bill of Lading will prevail.
PDF version of the STC is available through this link and the Terms and Conditions of Hecny House Bill of Lading is available on this link.
****
****

Personal Use

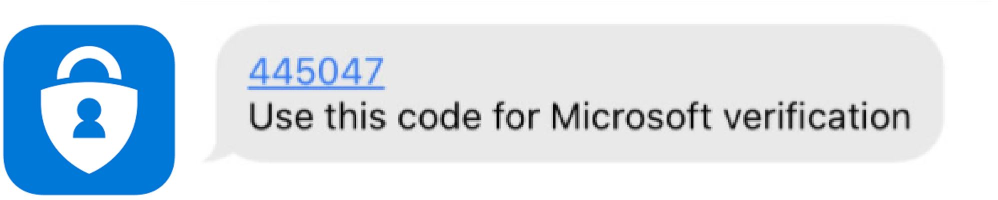
- Company E-mail services may be used for incidental personal purposes provided that such use does not:
  a) Directly or indirectly interfere with the Company operation of computing facilities or E-mail services.
  b) Interfere with the E-mail users' employment or other obligations to the company.
  c) Violate this Policy, or any other applicable policy or law, including but not limited to use for personal gain, conflict of interest or commitment, harassment, defamation, copyright violation or illegal activities.

Confidentiality

- The confidentiality of E-mail cannot be assured, and such confidentiality may be compromised by access consistent with applicable law or policy, including this Policy, by unintended redistribution, or due to current technologies inadequate to protect against unauthorized access. Users, therefore, should exercise extreme caution in using E-mail to communicate confidential or sensitive matters, and should not assume that their E-mail is private or confidential.
- Users may not access, use, or disclose personal or confidential information without appropriate authorization, and must take necessary precautions to protect confidentiality of personal or confidential information encountered in the performance of their duties or otherwise.

Security and Preservation

- E-mail to users and operators must follow sound professional practices in providing for the security of E-mail records, data, applications programs, and systems programs under their jurisdiction.
- Users and operators must guard against storage media deterioration and rapid technological changes which render E-mail records inaccessible due to hardware or software obsolescence.
- Users are responsible for safeguarding their identification (ID) codes and passwords, and for using them only as authorized.
- Office 365 users may use the multi-factor authentication self-enrolment process to register their authentication device(s) and install the Mobile app, the preferred ways for delivering verification codes are Mobile SMS or Mobile app (Microsoft Authenticator app).



445047
Use this code for Microsoft verification

Violations

- Suspected or known violations of policy or law should be confidentially reported to the appropriate supervisory level for the operational unit in which the violation occurs.

Exceptions

- Any exception to the policy must be approved by the of the appropriate company supervisory or management (i.e. Top Management, department heads, station managers.) in advance.

General Use Cautions

- The ability of a recipient to forward a message, or accidentally respond to a list rather than an individual, may broadcast an E-mail message widely.
- Remember that there is no way to guarantee that the purported sender of an E-mail message was in fact the real sender of the message. It is relatively easy to disguise an electronic identity.
- Printed E-mail Official Records should follow the hard-copy record retention and disposition schedules.
- Public Records are much more broadly defined than Official Records and may be considered to include, in certain circumstances, any information including all E-mail produced or received on company provided systems. Public Records, including E-mail, may be subject to disclosure under state public records law; or other applicable law, including by subpoena.
- Do comply with all Local laws and ethics.
- Do follow the normal standards of professional courtesy and conduct.
- Do respect copyright, proprietary rights, privacy laws.

You may not do

- Access, read, use, transfer or tamper with accounts or files that you are not authorized to use.
- Alter system software or hardware configurations without authorization.
- Libel or otherwise defame others via E-mail.
- Participate in illegal activities such as making threats, harassment, theft, breaching security measures, or violating other applicable law or policy.
- Engage in commercial activities not approved by the appropriate party and Top Management.
- Engage in activities for personal financial gain except as permitted under applicable company policies.
- Violate company policies and guidelines.
- Send or forward chain letters, letter-bombs or spam.
- Please DO NOT OPEN any uninvited documents such as PDF, Excel, Words and email! Never click on links inside those documents unless verifying the source.
- Never do money transfer before you verify the request. (You must call the sender!)
- Avoid clicking on malicious links. For example, if the domain of the link to which you are being directed doesn't match the purported company domain, then the link is a fake.

Permitted Use of Internet and Company computer network

The computer network is the property of The Company and is to be used for legitimate business purposes. Users are provided access to the computer network to assist them in the performance of their jobs. Additionally, certain Users may also be provided with access to the Internet through the computer network. All Users have a responsibility to use The Company's computer resources and the Internet in a professional, lawful and ethical manner. Abuse of the computer network or the Internet, may result in disciplinary action, including possible termination, and civil and/or criminal liability.

HECNY provides staffs with Internet access within the workspace, which can be setup as wired or wireless connection. Staffs with Personal Computer may have on-site access to the Internet.

Authorized Use

HECNY Group's Internet connection is intended primarily for business use. That means we expect you to use your Internet access primarily for business-related purposes, i.e. to communicate with business partners and other staffs, to research relevant topics in freight and logistics industry, as well as market trend, so as to obtain useful information. The following are specific provisions regarding authorized use of HECNY Group's Internet connection:

- Users may use the organization's Internet services for personal improvement provided that such use is consistent with professional and business conduct.

- Internet use should be restricted to sites and materials such as news or information that might be considered reasonable if read as a text publication in the working environment.

Unauthorized use

Users shall not use HECNY Group's Internet or E-mail services to view, download, save, receive, or send material related to the following:

- Offensive content of any kind, including pornographic material.
- Propagate a virus, worm, Trojan horse, ransomware or trap-door program code.
- Disable or overload any computer system or network.
- Circumvent any system intended to protect the privacy or security of another user.
- Promoting discrimination on the basis of race, gender, national origin, age, marital status, or disability.
- Visiting web sites that promote threatening or violent behaviour.
- Using the Internet for illegal activities including the illegal downloading of music, movies, or other copyrighted materials.
- Distributing Chain messages.
- Gambling web sites.

The above list of prohibited actions is by way of an example only and is not intended to be exhaustive.

Further, at all times users are responsible for the professional, ethical and lawful use of the computer system. Personal use of the computer is a privilege that may be revoked at any time.

User accountability

Users are responsible for their Internet use and are accountable for the following:

- Honoring acceptable use policies of networks accessed through the organization's Internet services.

- To have acceptable anti-virus software installed on any machine connected to the HECNY network. Examples of acceptable anti-virus software include products from Kaspersky (other software may also be appropriate). The software must have an active definition subscription.

- Users may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of the company.

- Unless expressly authorized to do so, Users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to The Company. Unauthorized dissemination of such material may result in severe disciplinary action as well as substantial civil and criminal penalties under State and country laws.

Privacy and monitoring

HECNY Group has software and systems in place to monitor and record all Internet usage. Our security systems are capable of recording each Web site and Email into and out of our internal networks. We reserve the right to do so at any time.

Employees are given computers and Internet access to assist them in the performance of their jobs. Employees should have no expectation of privacy in anything they create, store, post, send or receive using the company's computer equipment. The computer network is the property of The Company and may be used only for Company purposes.

Accidental/unintended violations

HECNY Group does use independently supplied software and hardware that provides data to identify inappropriate or sexually explicit Internet sites. We may block access from within our networks to all such sites. If you find yourself connected accidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program. A user who accidentally accesses a prohibited site is encouraged to report the incident to the company’s IT Department without the threat of incurring a violation penalty.

Violation penalties

Violations will be reviewed on a case-by-case basis. If it is determined that a user has violated one or more use regulations, that user will receive a reprimand from the Department Heads and his or her future Internet use will be closely monitored by I.T. department. If a gross violation has occurred, the Department Head will take immediate action. Such **action may result in losing Internet privileges, or other discipline as outlined in t**he Employee Handbook.

Blocking Sites with Inappropriate Content

Hecny has the right to utilize hardware and software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

Blocking Sites with Non-productive Content

Hecny has the right to utilize hardware and software that makes it possible to identify and block access to Internet sites containing non-work-related content such as (but not limited to) Drug Abuse; Hacking; Illegal or Unethical; Discrimination; Violence; Proxy Avoidance; Plagiarism; Child Abuse; Alternative Beliefs; Adult Materials; Advocacy Organizations; Gambling; Extremist Groups; Nudity and Risqué; Pornography; Tasteless; Weapons; Sexual Content; Sex Education; Alcohol; Tobacco; Lingerie and Swimsuit; Sports; Hunting; War Games; Online Gaming; Freeware and Software Downloads; File Sharing and Offsite Storage; Streaming Media; Peer-to-peer File Sharing; Internet Radio or TV; Internet Telephony; Online Shopping; Malicious Websites; Phishing; SPAM; Advertising; Brokerage and Trading; Web-Based Personal Email; Entertainment; Arts and Culture; Education; Health and Wellness; Job Search; Medicine; News and Media; Social Networking; Political Organizations; Reference; Religion; Travel; Personal Vehicles; Dynamic Content; Folklore; Web Chat; Instant Messaging or IM; Newsgroups and Message Boards; Digital Postcards; Education; Real Estate; Restaurant or Dining; Personal Websites or Blogs; Content Servers; Domain Parking; Personal Privacy; Finance and Banking; Search Engines and Portals; Government and Legal Organizations; Web Hosting; Secure Sites; or Web-based Applications.

Acknowledgement of Understanding

I have read and agree to comply with the terms of this policy governing the use of The Company's computer network. I understand that violation of this policy may result in disciplinary action, including possible termination and civil and criminal penalties.

Employee Name: ____

Employee Signature: ____