ISSUED BY: IMC	**IMC IT POLICY & GUIDELINES FOR END USERS**	
		Effective Date : 1st July 2022
		Version : 5.4

TABLE OF REVISIONS

Revision No.	Description of change	Section	Date
0.0	Launch of IT policies, guidelines & procedures for end-user computing	A. IT Policy For End Users	01 May 2004
1.0	Added new policies – IT-07 to IT-013	A. IT Policy For End Users	01 Dec 2005
2.0	Major changes implemented for IT-11 New IT System Request	A. IT Policy For End Users	01 May 2009
3.0	Restructure and implement End-User Computing Policies & Guidelines for IMC Group	A. IT Policy For End Users	15 Dec 2010
4.0	All sections were updated to align terminology for application to IMC Group. Topics from Section A “IT Policy for End Users” which are related to Business Applications under a new section “Group IT Policy for Business Applications”.	All sections	01 Jan 2014
5.0	All sections updated to align with the latest technology deployment. Also to remove Section B and C to be reorganized into IT Ops manual separately. Added new section for IMC Cyber Security Policy and guideline	All Sections	16 Apr 2019
5.1	Updated to allow email message from 30MB to 100MB	ITP-EU-02 : EMAIL 5.4.2	21 Nov 2019
5.2	Rebased as an IMC Group Policy applicable to the IMC Group of companies Added guidelines for email fraud prevention	ITP-EU-02 : EMAIL Section 6	18 Jan 2021

5.3	Revision to Password Policy to set expiry to industry best practice of maximum 90 days.	ITP-EU-05: IT Security	28 Jun 2021
5.4	Updated IT procurement to provide standardized laptop for all eligible staffs. Desktop will only be provided on exception basis with approval from Business Unit head. This is to support hybrid work arrangement. Added Choose Your Own Device guideline.	ITP-EU-04: IT Procurement	1st July 2022

POLICY REVIEW AND APPROVAL

Proposed By	**Reviewed By**
Cheong Luen ________________________________ **Cheong Wai Luen** **Director, IT** **IMC Group**	________________________________ **Oon Chen Yen** **Head, Group Risk Management** **IMC Group**
Approved By	
________________________________ **Richard Lai** **Group CFO** **IMC Group**	________________________________ **Loh Niap Juan** **Chief Corporate Officer** **IMC Group**

TABLE OF CONTENTS

1 OBJECTIVES

1.1 Information technology resources of the IMC Group (the “**Group**” or “**IMC**”) are provided to support the Group’s business and operational activities. Inappropriate and ineffective use of IT equipment, systems and services leads to wastage of IT resources and exposes the Group to various risks, including virus attacks and loss of data, compromise of the security of computer systems and potential legal issues.

1.2 This IMC Group IT Policy and Guidelines for End Users (the “**IMC IT Policy For End Users**”) is established to provide the essential principles, directives and guidelines to ensure:

- the authorized and lawful use of IT equipment, systems and services of the Group; and
- the effective and efficient use of these IT resources within the Group.

2 GOVERNING POLICY

2.1 The IMC IT Policy for End Users shall be the overall governing policy for all units/companies within IMC, subject to any applicable local legal and statutory regulations or requirements.

2.2 In line with the IMC Group Policy Guidelines, IMC SBG (Strategic Business Group) Corporate Offices may adapt and enforce a business-specific IT policy as required for their respective SBGs or SBUs (Strategic Business Units) in line with applicable local legal and statutory regulations or requirements. Any adaption or modification to the IMC IT Policy for End Users that are necessitated by such local requirements must be supported by written documentation with approval by IMC Group IT and such other approvals as may be required by the IMC Group Policy Guidelines. The adapted SBG or SBU specific IT policy is to be lodged with the repository of IMC Group Policies posted on IMConnect (or such other platform as may be applicable from time to time).

2.3 This IMC IT Policy for End Users and all individual IMC SBG or SBU IT policies that are issued pursuant to it are to be governed and enforced by the respective SBG management.

2.4 IMC Industrial Group IT (“**IMC Group IT**”) is the Document Owner of this IMC IT Policy for End Users.

3 DEFINITIONS AND SCOPE OF POLICY

3.1 The IMC IT Policy for End Users are applicable to all staff and visitors of companies within the Group.

3.2 “**Staff**” refers to all employees (permanent, contract and temporary), trainees, student placements and interns, of companies within IMC.

3.3 “**Visitors**” refers to all external personnel such as contractors, consultants, auditors, agents, and vendors.

3.4 “**IT equipment**” refers to all company-issued computers (eg. desktops, notebooks), smartphones, peripherals (eg. printers, scanners), storage devices (eg. external hard disks, USB flash drive), including the licensed software installed in such equipment.

4 CONTENTS

4.1 The IMC IT Policy and Guidelines cover key aspects of IT which are applicable to End Users, as set out in the documents listed below.

Document Number	Document Name
ITP-EU-01	Network and Internet
ITP-EU-02	Email
ITP-EU-03	Software
ITP-EU-04	IT Procurement
ITP-EU-05	IT Security
ITP-EU-06	Virus Management
ITP-EU-07	Remote Access
ITP-EU-08	IT Helpdesk & Incident Management
ITP-EU-09	Cybersecurity

5 COMPLIANCE

5.1 All staff and visitors are required to comply with the IMC IT Policy for End Users. Staff are responsible to communicate the applicable IT policy and guidelines to their visitors who require the usage of the Group's IT equipment, systems, and services.

5.2 IMC Group IT and the respective IT Departments for each SBG/SBU/Business Unit will regularly monitor and conduct annual compliance checks for compliance with the IMC IT Policy for End Users and any SBG or SBU specific IT policy that may be issued pursuant to the IMC IT Policy for End Users.

6 VIOLATION OF POLICY

6.1 Any staff who violates the IMC IT Policy for End Users or otherwise abuses the privileges of accessing and using the Group's IT equipment and services will be subject to disciplinary and corrective action, including loss of IT privileges, disciplinary actions and, in serious cases, up to termination of employment.

7 CONTACT & REVIEW

7.1 The IMC IT Policy for End Users will be reviewed by IMC Group IT annually and on an ad-hoc basis if required.

7.2 IMC Group IT reserves the right to change the IMC Policy for End Users at any time.

7.3 For clarification of any issue pertaining to the IMC IT Policy & Guidelines, staff are to contact IMC Group IT or their respective Business Unit's IT Department.

1 OBJECTIVE

1.1 This purpose of this document is to specify the policy, directives and guidelines to ensure the proper use of the IT network and the internet services provided by IMC.

2 DEFINITION

2.1 Network and Internet Services include but are not limited to the following :

- Network file and print services
- Internet surfing
- Instant messaging
- Peer-to-peer services
- Voice-over-IP and Video-over-IP
- File transfers (downloading and uploading of files)
- Access to Internet-based news, research, and other information services

3 PRIVACY POLICY

3.1 Staff are granted Internet access for work-related usage purposes, such as information gathering, research and online submission of documents and data via the internet.

3.2 IMC has the right to monitor all aspects of its computer systems usage and network traffic.

3.3 Monitoring of computer systems usage and network traffic includes, but is not limited to, the monitoring of websites visited by staff and visitors on the Internet, blocking of access to websites deemed inappropriate, and monitoring of materials created, stored, sent or received by staff on IMC's network.

4 INTERNET ACCESS AND USAGE POLICY

4.1 Offensive material and inappropriate websites: Staff are strictly prohibited from accessing websites or downloading/uploading material that is sexually explicit, profane, obscene, harassing, racially or religiously offensive, and defamatory, constitutes an illegal threat or violates any applicable company policy.

4.2 Staff are not to download other prohibited or restricted materials, which include but are not limited to, materials which are protected by copyright, trademark, trade secret or other intellectual property rights.

4.3 By default, downloading of all executable files will be blocked. If such files are required for work-related purposes, staff are to contact the respective IT Department for their Business Unit for assistance.

4.4 Staff are prohibited from downloading games and other entertainment software, play games over the Internet, participate in chat-rooms and inappropriate online forums, carrying out FTP file transfers with non-work related sites.

4.5 Staff are prohibited from uploading company information to the Internet, unless prior approval has been granted by the relevant level of Management.

4.6 Staff are to restrict distribution of their company-issued email address to websites for work-related purposes only, such as those belonging to vendors, service providers, and customers.

4.7 Staff are not to use company-issued email addresses to post comments or information on forums, personal websites or subscribe to any social networking websites.

1 OBJECTIVE

The purpose of this document is to specify the policy, directives and guidelines to be followed in order to ensure the proper use of company email and to protect the confidentiality of the Group's email records.

2 Usage of Email and Email System

2.1 IMC considers email as an important means of communication both within the organization and with external parties. Email services provided by IMC shall be used by Staff for communication of business and work-related activities and internal company matters only.

2.2 It is the responsibility of all Staff to ensure that the email system is used properly and that a professional image is projected at all times when communicating with external parties.

2.3 In particular, Staff are not to:

- send or forward any email containing offensive, racist, political or obscene contents;
- send or forward any chain letter or junk mail;
- mass-mail any non-work related messages;
- send email messages using another staff's email account in order to impersonate the staff;
- disguise or attempt to disguise their identity when sending emails;
- circulate or distribute games, screensavers, or other non-work related programs which can disrupt or congest the email service or network;
- delete, destroy, encrypt or remove any email messages which causes disruption, damage, or harm to the business, operations or reputation of the company.

3 Company Emails on Personal Devices

3.1 Personal mobile devices include, but are not limited to, mobile internet devices, mobile phones, smartphones, mobile or tablet computers, and personal digital assistants (PDAs).

3.2 For improved productivity, staff are allowed to access their company issued email account on company issued personal mobile devices using the application as dictated by IMC Group IT. For non company issued personal mobile devices, only the Microsoft Outlook app is to be used for accessing email.

3.3 Any authorization for staff to receive company emails on a non company or company issued personal mobile device is subject to the staff irrevocably authorizing and granting IMC the right to access, inspect, make copies of and/or remove all contents, whether work or non-work related, on the personal mobile device.

3.4 Staff must immediately notify IMC in event of loss of the personal mobile device, in order that appropriate action (if any) may be taken to prevent or restrict disclosure of any proprietary information on the personal mobile device.

4 Email Monitoring

4.1 All messages distributed via and stored in IMC's email systems, including personal emails, are the property of IMC.

4.2 IMC reserves the right to monitor, inspect or review any and all emails stored, created, or received in the office email system without prior notification.

5 GUIDELINES

5.1 Accessing Email Remotely Using Non-Company IT Equipment

5.1.1 Staff are advised NOT to access office email via an internet browser from an external or non-company issued computers, such as an internet kiosk or a computer located at hotels, airports, and cyber cafes.

5.1.2 In event of work-related exigencies, and Staff need to use an external non-company issued computer to access their office emails, they are to exercise due care and take necessary precautionary actions, such as ensuring that they log-off from the email system and clearing the web browser temporary files, cookies, and history after the email activity is completed.

5.2 Use of Email Signature

5.2.1 The company considers the use of email signature a form of external branding.

5.2.2 Staff should follow the current guidelines issued by IMC Group Communications in order to standardize the content and format of the email signature. Email signatures should not have a tagline or a slogan.

5.2.3 Email signatures should have all or some of the following fields: name, designation/department, company name, address, telephone (main), telephone (DID), mobile number, fax number, email address, and website address.

5.2.4 Business unit heads should write to IMC Group Communications in Singapore Office if they need any clarifications or for consideration and approval for any deviation from this policy.

5.3 Email Account Guidelines

5.3.1 Each Staff is assigned one or more email accounts, which will be used for business and work-related communications. Based on the nature of the business and role of the staff, the incoming and outgoing messages may be duplicated in a shared email directory.

5.3.2 The following are guidelines on email accounts applicable to offices that manage their own email server:

- By default, each email account will be allocated a fixed amount of storage space in the email system.
- The email system will issue a warning when any of the mailboxes reaches the threshold value.
- If Staff do not heed the warning and take proper housekeeping action, the email account which exceeds the storage limit will not be able to send new messages.

- All Staff are to housekeep and maintain their email accounts to ensure that the storage space allocated is not exceeded. This can be done by:
  - Archiving messages to personal email folders located on the workstation
  - Regularly backing up their personal email folders to external backup devices or on other storage locations as provided by the company
  - Deleting unwanted or expired email messages. Emptying the “Deleted Items” folder regularly.
- Maximum message size for each incoming and outgoing message communicated with an external party will be set. The current incoming and outgoing message size is 100MB.

6 Fraud prevention

6.1 It has become prevalent for many fraudulent schemes to be carried out over email. Staff are to stay vigilant when conducting their business over email. The following guidelines are to be complied with:

6.1.1 Do NOT click on link from unknown sender. Always check the email address carefully for mis-spelling.

6.1.2 Do NOT key in your username and password on unknown website. Always check the URL address carefully to ascertain legitimate website.

6.1.3 Be aware of the technologies deployed to detect phlishing email and do NOT ignore any warning from the system.

6.1.4 Always check with sender via non email means or IT Department if in doubt over any specific email.

ISSUED BY: IMC	IMC IT POLICY & GUIDELINES FOR END USERS	
	ITP-EU-03 : SOFTWARE	Effective Date : 1st July 2022
		Version : 5.4

1 OBJECTIVE

1.1 The purpose of this document is to specify the policy, directives and guidelines to ensure the proper management and usage of IT software.

2 Usage of Software

2.1 Licensed Software

2.1.1 IMC will, and expects all staff to, strictly comply with prevailing Copyright laws and software vendor licensing terms.

2.1.2 Only authorized and licensed software are to be installed at all times.

2.1.3 Software authorized for use include:

- software purchased by the company through the requisition process;
- software which is bundled as an integral part of the IT equipment;
- software legally transferred through a software license transfer process;
- software developed by the IT Department or appointed software vendors; and
- Opensource that is licensed under respective license agreement.

2.2 Staff are strictly not allowed to install and use illegal, unlicensed or unauthorized software in company-issued computers. Staff are also not to make an unauthorized copy of any software program which is installed on the computer.

2.3 All legal and licensed software installed on company-issued computers is to be used for work purposes only.

2.4 Staff who require use of software licensed by the company on personal computers at home must consult with the IT Department of their respective Business Units to ensure that such use is permitted by the software licensor.

2.5 Any staff found making unauthorized copies of software or installing and using illegal or unlicensed software will be personally liable to any proceedings and subject to further action as deemed necessary by IMC.

2.6 Software on Computers

2.6.1 All software must be authorized by the IT Department of the respective Business Units before they can be installed on computers.

2.6.2 Staff are to contact the IT Department at their respective Business Units for all other software applications which may be required on their computers.

2.6.3 All new software purchase and installation are to be reviewed jointly by the Business Unit and respective IT Department with final approval from head of IMC Group IT.

1 OBJECTIVE

1.1 The purpose of this document is to set out the policy, directives and guidelines to ensure that IT procurement is carried out in a cost-effective manner which is compliant with the applicable authority manual and in accordance with optimal standards so as to deliver best overall value for the Group.

2 DEFINITION

2.1 IT Items refer to hardware, software, and IT-related services, including but not limited to the following:

- Computers (e.g. desktop computers, notebooks)
- IT peripherals (e.g. keyboards, display panels, printers, scanners, CD/DVD- writers)
- Backup software and backup devices
- Servers, storage, and related software
- Computer room equipment such as uninterruptible power supply units, air- cooling systems
- Database licenses
- Software applications
- Consultancy and advisory services for IT
- Software development manpower services
- Subscriptions to 3rd-party hosted IT systems

3 POLICY

3.1 Company managed computer (Non-CYOD scheme, for CYOD scheme see Section 3.2)

3.1.1 Issuance of Computers

3.1.1.1 Staff will be issued a notebook based on computing requirements of their responsibilities and requirements:

3.1.1.2 Job grade with Associate Director and above;

3.1.1.3 Staff that require to work from home;

3.1.1.4 Staff that only works in the office.

3.1.1.5 Issuance of Desktop would be strictly on an exception basis and subject to approval of the relevant Business Unit Head.

3.1.1.6 The model and specification of the assigned device are to be standardized by IT Department for efficient maintenance and internal equity. These standardized model would be refreshed on a periodic basis. Any exception is to be granted by SBG management.

3.1.1.7 If there is an existing computer within the Business Unit, then the staff will be issued the item. Otherwise, IT Dept will advise the staff to raise a Purchase Requisition for the purchase of a new computer.

3.1.2 Replacement of Computers

Desktops and notebooks will be replaced only after 3 years' of asset-life (from date of purchase) or when computer equipment component failure occurs and is assessed to be beyond economic repair.

3.1.3 Procurement Authority and Approval

- The approving authorities for IT requisition and procurement shall be in accordance with the relevant Authority Manual applicable to the Business Unit.
- All procurement of IT items shall be processed by the IT Department for that Business Unit.
- In addition, a check must be made against IT equipment spares held by various Business Units which are supported by the IT Department. If equivalent spare equipment is available and the asset-owning Business Unit and Requestor agrees to transfer of the item, then arrangements will be made for the spare equipment to be used and new item purchase will not be made.

3.2 Choose Your Own Device (CYOD)

3.2.1 The Choose Your Own Device guidelines will apply only to countries where the CYOD scheme has been implemented.

3.2.2 The CYOD scheme is an important element in the new hybrid workplace that enables greater flexibility in how, where and when we work and collaborate. This is supported by the on-going transformation to cloud based applications and technology.

3.2.3 With the CYOD scheme, staff will be able to procure (on a reimbursement basis) and use devices of their own choice, subject to adherence with the CYOD guidelines herein and to this Group IT policy.

3.2.4 While the CYOD device is owned by staff, it is important that the following are adhered to:

- CYOD devices are not to be shared with any person that does not work in any IMC Group company (including family members).
- CYOD devices are subject to company monitoring of communications, network traffic and browsing history.
- Company has the right to review or inspect and retain company related data on the CYOD device. Any data that is subjective would be considered as company related data.
- Company data that resides on the CYOD device remains company's property. Employees have the responsibility to ensure that both data and device are protected at all times.
- Company may remotely wipe the data off the CYOD device.
- Report the loss of the CYOD device immediately to local IT helpdesk so that appropriate action can be taken to safeguard company and/or personal data expeditiously.
- Company will not responsible for loss or damage to personal application or data resulting from the use of company applications or remote wipe of data.

3.2.5 Staff are to take full responsibility for the availability and performance of the CYOD device to support their assigned duty and work.

3.2.6 The purchase of the CYOD device can only be reimbursed every 3 years from the last date of reimbursement where applicable. Newly joined employees can get reimbursement from their first day of work. The maximum amount that can be reimbursed is subjected to local IMC policy.

3.2.7 Staff are strongly encouraged to procure their CYOD device with at least 36 months of warranty that covers service and part replacement.

3.3 IT Systems & Software Development Policies

- All requests for purchase of IT items, including IT equipment, software applications, and software development services, must be routed to the IT Department for review and approval.

- All enterprise software application supporting the business operation directly would need to be jointly reviewed by the respective IT Department and the Business Unit with final approval from the Head of IMC Group IT.

4 GUIDELINES

4.1 IT Equipment Standards & Configuration

- IT Department will specify the list of standard equipment makers/brands, equipment configuration and the prevailing estimated prices for the purchase of new desktops, notebooks, and peripherals such as printers and monitors. The list is reviewed and updated by IT Department on an annual basis, or as and when there are significant changes to the product pricing.
- The key benefits of equipment standardization include better product pricing, lower cost of support and to ensure interoperability of systems.
- All IT items procured shall comply with the prescribed standards and configuration.
- Any request for a deviation from prescribed standards and configuration will be reviewed and approved on a case-by-case basis by Functional head/SBG head/Country Head.
- Staff are to contact their respective IT Department for their Business Unit for details of recommended equipment configuration and estimated pricing.

1 OBJECTIVE

1.1 The purpose of this document is to specify the IT security policy, directives and guidelines to protect the Group's assets and prevent unauthorized access to the Group's systems and information.

2 POLICY

2.1 Network/System User-ID/Email and Password

2.1.1 IMC adopts the Principle of Least-Privilege (PLOP) model in enhancing the protection of data and functionality from faults and malicious behavior, among other attacks. Staff should log on with a user account that has the absolute minimum permissions necessary to complete the current task and nothing more. This principle applies to computers and the use of those computers. Use of Administrator Access should be consistent with an individual's role or job responsibilities as prescribed by management.

2.1.2 Each staff is assigned a unique network user ID and email account by the Systems Administrator. The creation of new accounts for staff will be carried out only upon notification by the P&O Department.

2.1.3 Staff who are assigned a network user ID and email account are directly responsible and accountable for the usage and to safeguard the accounts. Staff are to ensure that the assigned network user ID and password are kept confidential and not shared with others, including colleagues or team members.

2.1.4 Staff are to change the password on a regular basis, and whenever the need arises. This will prevent any misuse or unauthorized use of the staff user-ID and email account.

2.1.5 If it is suspected that a password has been compromised or 'leaked' to another person due to various reasons, staff should take action and change it immediately.

2.1.6 The current password policy is 90 days, with minimum 10 characters and with password complexity enabled.

2.1.7 All password is to follow the password complexity policy as follows:

- Between 10 and 128 characters long.
- Use at least 3 of the following types of characters: (a) uppercase letters, (b) lowercase letters, (c) numbers, and/or (d) special characters.
- Password must be unique and last 3 passwords cannot be re-used.

3 Company-issued IT Equipment and Information Protection

3.1 Staff who are assigned IT equipment to work with are directly responsible and accountable for the equipment and the information stored within the equipment.

3.2 Staff are responsible to regularly back up their working documents and email files which are stored locally on the IT equipment. Data are to be backed up onto file servers as provided by IMC for this purpose or to cloud via company issued OneDrive only.

3.3 Staff are to store work-related data and documents on the office network file server or company sharepoint so as to minimize the risk of data loss.

3.4 Staff must report any loss or theft of company-issued computers, handheld devices, smartphones or other IT equipment immediately to their BU/Department Head as well as IT, Administration and Insurance Departments.

3.5 Upon investigation, if the loss or theft is found to be due to the negligence of staff, he/she may be held responsible and accountable for the cost of replacement of the item/s.

3.6 All IT equipment issued by the company is to be used for company and work-related purposes only. Staff are to refrain from storing non-work related and personal files in the company-issued IT equipment.

3.7 All contents stored in company-issued IT equipment are the property of IMC and staff shall assert no rights over the contents in any IMC-issued IT equipment.

3.8 Any act of Staff (including but not limited to adding, editing, copying, forwarding, and deletion of file and records from databases, and files from shared folders and company-issued IT equipment) which causes disruption, damage, or harm to the business, operations, and reputation of IMC shall be deemed to have violated company policy and the relevant disciplinary and other actions will be taken by IMC.

3.9 IMC reserves the right to monitor the usage of IT equipment, both as it occurs and in the form of account histories and their content. Monitoring and inspection can be carried out through the use of automated software.

3.10 IMC has the right to retrieve and inspect any and all files stored in the IT equipment issued by IMC.

3.11 IMC has the right to remove any personal and non-work related files found in the IT equipment issued by IMC.

4 IT Equipment on Company Premises

4.1 IMC reserves the right to monitor the usage of all IT equipment (including personal IT equipment) on company premises, both as it occurs and in the form of account histories and their content. Such monitoring and inspection can be carried out through the use of automated software.

4.2 Staff irrevocably authorizes and grants the company the right to access, inspect, make copies of and/or retain any personal IT equipment and its contents that are brought onto company premises.

5 Use of Non-Company Issued Workstations in Office

5.1 Unless approval from BU/Department Head and IT Department has been granted, non-company issued external workstations shall not be connected to the office network. This directive is in place for the following reasons:

- Virus version control and management will be compromised;
- Software licensing and accountability of staff becomes vague;
- Information will be easily copied and will reside in non-company issued devices;

- IT support issues may arise due to non-compliance with company policies and guidelines.

6 Employee Resignation or Termination

6.1 Staff must return or account for all IMC-issued IT equipment with their respective BU/Department Head and IT Department before he/she leaves IMC.

6.2 Staff and respective BU/Department Head must also ensure that all company information stored on authorized non- company issued workstations or storage devices (if applicable, due to work or business reasons) are completely removed before he/she leaves IMC.

7 GUIDELINES

7.1 Safeguards for Information Access

7.1.1 Users should configure their workstations to automatically lock after a period of inactivity to prevent unauthorized access to company data. It is recommended to set the period as 15 minutes.

7.1.2 Below are some recommended guidelines for the management of passwords:

- Do not use a commonly-used word such as “password”, “mouse” or any word found in dictionary (English or foreign), word or number pattern such as “123456”, “111”, “asdfgh”, “aabbcc”, “abc123”, date of birth or other personal information;
- Avoid using the same password for all login accounts or repeat old passwords;
- Length of passwords should be at least 10 characters long;
- Password should not be written down or stored online.

7.2 Safeguards for IT Equipment

7.2.1 Below are recommended guidelines to protect IT equipment and data :

- All removable storage media with data should be kept in a locked environment when not in use;
- A notebook locking device should be used to secure a notebook when working in an open cubicle;
- IT equipment should not be left unattended in public places;
- IT equipment should not be placed in exposed areas within the motor vehicle so as to minimize theft;
- An inventory record of removable storage media issued to the staff should be maintained so that issued items are accounted for upon resignation or termination of the staff;
- Company data should not be transferred or copied to a non-company issued device or computer unless it is authorized for work-related purposes. Data must be deleted from the equipment upon the conclusion of the work-related activity.

1 OBJECTIVE

1.1 The purpose of this document is to specify the policy, directives and guidelines to ensure the effective and proactive management of potential computer viruses, and that appropriate measures are taken to manage and recover from virus infections.

2 POLICY

2.1 Anti Virus Software

2.1.1 All company-issued computers shall be installed with an anti-virus software.

2.1.2 Staff are not to uninstall, turn off or disable the real-time anti-virus software. When in doubt, staff should consult with the IT Department of their Business Unit for clarification.

2.2 Non-work Related and Unauthorized Software

2.2.1 Staff are not to install, execute or distribute any non-work related and unauthorized software on office computers. This includes third-party screen savers, games and other such software programs as they carry a high risk of being 'Trojan Horses' or malicious programs designed to destroy data or allow external unauthorized access to office systems and resources.

2.2.2 Staff are also not to download non-work related software programs from the Internet or circulate such programs through the email system.

2.2.3 The use of peer-to-peer internet connection or file-sharing software is strictly prohibited.

3 GUIDELINES

3.1 Preventive Measures

3.1.1 Computers which have not been connected to the office network over a period of time should be scanned for viruses with the latest pattern file before connecting to the network.

3.1.2 Staff are to be alert when receiving emails with suspicious titles or sender address.

3.1.3 If it is suspected to be a virus-infected email, contact local IT Department for verification and advice.

3.1.4 All virus-infected emails should be immediately deleted, and trash bin (deleted items folder) set to "Empty". Note that viruses are able to generate emails which appear very authentic, such as bearing the office email domain name as the sender.

3.1.5 Staff are not to open or download links or attachments contained in emails from unknown, suspicious or untrustworthy sources. These attachments should be deleted immediately, and emptied from the trash bin (deleted items folder).

3.1.6 Staff are not to forward spam, chain and other junk emails.

3.1.7 Staff should always scan all external media (e.g. thumb drive or any removable storage) and downloaded files for viruses before use. Use of externally mounted storage media is not encouraged.

3.2 Assistance and Alerts for Computer Virus Attacks

3.2.1 To limit the spread of a virus attack, early notification and co-operation are required from all staff.

3.2.2 In the event of a major virus outbreak, the IT Department will circulate a virus alert for potential or dangerous viruses. Patches and virus fixes will be executed when necessary. These may cause performance degradation on the computers. In some cases, the IT Department will need to disconnect computers from the network to isolate the problem.

3.2.3 Staff who are uncertain whether a virus warning received from an external source is authentic or a hoax email are advised to contact the IT Department for clarification and assistance.

3.2.4 Staff are not to forward external emails which contain virus warnings.

3.3 Recovery and Isolation From Virus Attacks

3.3.1 In the event of a confirmed or suspected virus attack on the computers, the staff are to :

- Immediately contact the IT Department of their Business Unit;
- Log off and disconnect the computer from the office network in order to prevent the virus from spreading to other computers.
- IT Department will help to scan the infected computer and take corrective actions as required

1 OBJECTIVE

1.1 The purpose of this document is to set out the policies, directives and guidelines for remote connection to the Group's office network so as to protect the systems and information of the Group.

2 POLICY

2.1 Approval For Remote Access

2.1.1 Only authorized staff will be permitted to remotely connect to the required company IT systems, networks and data repositories.

2.1.2 Requests for grant of remote access rights and any changes to the access rights must be approved by the BU/Department Head of the Staff before submission to the IT Department.

2.1.3 The request form will include staff details, the effective start date for the grant of access and the specific modules, capabilities or categories to be granted to the staff and any other pertinent information.

2.1.4 Staff are responsible for safeguarding the assigned user ID and password for remote access and for all transactions made with the remote access user ID and password. Multi-factor authentication needs to be implemented for cloud-based access.

2.2 Remote Access Usage

2.2.1 Staff who have been granted remote access rights and issued with remote access account IDs shall be solely responsible for all activities performed by their user account remotely. They are also to be responsible for the safekeeping and usage of the account ID and password.

2.2.2 The account ID shall be utilized only by the staff and must not be shared with any other persons, including their office colleagues.

2.2.3 Staff are to promptly disconnect the computer from the remote connection after usage.

2.3 Software Requirements

2.3.1 A remote connection must be made through a secure, authenticated and centrally managed access method and software administered by IT Department.

2.3.2 Staff are to ensure that computers which are used to remotely connect to the company network have the following software installed and enabled:

- Anti-Virus software - The anti-virus is required to be operating on the computer at all times in real-time protection mode. The anti-virus library definitions must be the latest updated version
- Firewall - The computer must be protected by a firewall at all times when it is connected to the internet. Staff can use the built-in Windows firewall or other firewall software at their own discretion.

1 OBJECTIVE

1.1 The purpose of this document is to ensure proper reporting, investigation, and management of IT incidents so as to minimize potential adverse impact on business operations. In addition, the scope, procedures, and process for IT Helpdesk and the management of IT incidents is set out.

2 DEFINITIONS

2.1 An **Incident** is defined as an event that deviates from the expected standard operation of an IT service or system. An Incident can be detected by a user of a service/system or by staff within the IT Department.

2.2 **Incident Priority** is the sequence in which an Incident needs to be resolved, based on impact and urgency of the Incident.

2.3 The **impact** is the extent to which the Incident leads to deviation from the normal level of service provision.

2.4 **Criticality** reflects the time available for repair or resolution before the impact of the incident is felt by the business.

2.5 A **request** is defined as a user based request to have a specific requirement fulfilled that is not related to an incident.

3 POLICY

3.1 IT Helpdesk

3.1.1 The IT Helpdesk is the first point of contact for staff who require assistance with IT and IT-related matters.

3.1.2 Staff are to submit an IT request, post a query or report an incident, by placing a call, sending an email to the IT Department, or, where available, input the request to the IT Helpdesk website.

3.2 IT Helpdesk Personnel

3.2.1 IT Helpdesk personnel are responsible to carry out the following :

- Provide the first point of contact for staff who wish to report an IT incident, post a query or submit a service request;
- Provide IT support to staff via the telephone phone or by remotely taking control of the user’s PC (with their consent) for troubleshooting;
  - Log tickets to the IT Helpdesk System, where applicable;
  - Analyze incidents, prioritize and assign the incident to relevant IT Staff and/or Software Application User Administrator for 2nd level support;
  - Escalate incidents which cannot be resolved within the stipulated timeframe or beyond capabilities of 2nd level support to the vendor and IT management;
  - Ensures all incidents are followed up and closed.

3.3 Helpdesk Ticket Categories

3.3.1 IT Helpdesk tickets can be categorized as follows:

- Request – Request for clarification or query regarding the use of IT equipment, IT services or software application; including request for IT services such as setup of the computer for new joiner or installation of software on a computer;
- Incident – Problems encountered in the use of IT equipment, IT services or software application.

3.3.2 For a Request which can be directly handled by IT Helpdesk personnel, they will provide first level support by giving guidance and/or directing the user to the relevant information resources. For a request which is related to specific software applications or cannot be handled by IT Helpdesk personnel, the ticket is assigned to the relevant IT Staff from Applications Team or the Application System User Administrator who will provide guidance to the user as required.

3.3.3 For a request received, the ticket is assigned to an IT staff who will make necessary arrangements with users to service the request.

3.3.4 For an Incident, IT Helpdesk personnel will assess the impact and criticality, and assign an appropriate severity level to it. Head of IMC Group IT and Head of IT Department for the relevant Business Unit will be notified for severity level 1 incident. The table below shows the matrix of impact and criticality and assignment of severity levels from 1 to 3:

Business Impact/Criticality	Low	Medium	High
Low	3	3	2
Medium	3	2	1
High	2	1	1

3.3.5 A detailed description of the IT Incident Management Process is provided in the following section.

- An Incident is reported by either a user of a service/system or a staff from the IT Department. Incident reports are recorded by (a) sending an email to IT Dept or (b) contacting IT Helpdesk via telephone or in person, or (c) capturing the details in the IT Helpdesk System, where the system is available.
- Each Incident is assigned a Severity Level based on its Impact and Criticality. Based on the nature and source of the incident, it is assigned to one of the IT Staff or Application System User Administrator for investigation, diagnosis, and resolution, with the objective of minimizing disruption to business operations.
- Incidents which cannot be resolved internally by the IT Staff or Application System User Administrator are forwarded to the vendor for further investigation and resolution.
- Incidents related to 3rd party software applications are reported to the respective vendors for further resolution. IT Staff from Applications Team and the respective User

Administrator for the software application are responsible for monitoring the status of these incidents. They are to escalate the incident to IT Department and user management in event of a delay to the resolution of the Incident which will adversely impact business and user operations.

- Incidents related to IT infrastructure and systems such as firewall or servers will be reported to the respective vendor for the IT equipment or system. IT Staff from Infrastructure Team is responsible for monitoring the status of these Incidents. They are to escalate the Incident to IT management in event of a delay to the resolution of the Incident which will adversely impact business and user operations.
- All proposed resolutions, whether from the IT Department, User Administrator or from vendors, which require a change to be applied to the affected system must comply with the IT Change Request Policy.
- An Incident will be closed when a solution has been found and implemented.
- Staff who reported the Incident will be kept informed of the status of the resolution of the Incident.

1 INTRODUCTION

1.1 The purpose of this document is to provide directives and guidelines for protecting and preserving the security of IMC's data and technology infrastructure.

1.2 This document supplements Document ITP-EU-05 above on IT Security for further protection.

2 SCOPE

2.1 This document is complementary to any other IT policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices which may be issued from time to time by IMC Group IT.

3 NON-PUBLIC INFORMATION

3.1 The definition of Non-public information in the context of cybersecurity shall mean all electronic information that is not publicly available. All staff are obliged to protect the non-public information of IMC. Other key definitions are below:

- ***Company secret*** – any information that can derive independent economic value to individual or competitors, actual or potential, from not being generally known, and not being readily ascertainable through proper means by, the public or unauthorized employee. This would include company strategic plans, financial details as well as proprietary information such as copyrighted information and subject matter of patents.
- ***Personal Identifiable Information*** – any information that leads to the identification of personnel. This does not include publicly disclosed and business related personal information such as those readily available on public domain and business card. The collection, use, disclosure and care of personal data are governed by the operating country equivalent personal data protection regulation. In Singapore, it is governed by the Personal Data Protection Act 2012 (PDPA).
- ***Confidential*** – any information that is not generally available to employee or public that will cause undue disruption and prejudicial to the business. This information may or may not result in financial loss to the business. This would include product ideas, internal processes, and costings, shipping schedule, inventory position, customer database and relationships, budget and forecast, P&O personnel-related information.
- ***Restricted*** – any information that is used internally by an employee in the course of business but not available to the public.

4 PERSONAL AND COMPANY's DATA PROTECTION

4.1 When employees use their digital devices to access company emails or accounts, they introduce security risk to data. It is of importance that our employees keep both their personal and company-issued computer, tablet and mobile devices secure. The following practices are to be adhered to:

- Keep all devices password locked and protected when not in use;
- Ensure proper installation and setup of antivirus software;
- Ensure the devices are not exposed or unattended;
- Ensure that security updates provided by the software vendor are updates as soon as feasible;
- Only log into company accounts and systems through secured or private networks only.
- Do not access company internal systems from devices not owned by you or lend your devices to others.

5 EMAIL SECURITY

5.1 Email is a typical means for introducing or transferring scams, malware, ransomware, and malicious software (eg worms). The following practices are to be adhered to:

- Do NOT open attachments from an unknown sender. If in doubt, always call the sender to clarify.
- Do NOT click on links when the content is not adequately explained
- Always be suspicious of clickbait titles (e.g. offering prizes, advice);
- Always check the sender name and email address to ensure they are legitimate;
- Always look for inconsistencies or giveaways (e.g. grammar mistakes, capital letters, and excessive number of exclamation marks);
- If in doubt, please refer the matter to IT Helpdesk for further verification.

6 PASSWORD MANAGEMENT

6.1 The integrity and security of the individual password are important. Any leakage is hazardous as it may compromise our entire system security and integrity. All passwords are meant to be personal and secret. The following practices are to adhere to:

- Use passwords with at least 10 characters (including capital and lower-case letters, numbers, and symbols) and avoid information that can be easily guessed (e.g. birthdays);
- Always remember your password mentally and do NOT write them down on paper.
- Always change your passwords regularly. The system policy enforces password change every 6 months.

7 DATA TRANSFER SECURITY

7.1 Avoid transferring sensitive data (e.g. customer information, employee records) to other devices or accounts unless absolutely necessary.

7.2 Only share confidential data over the company network or secured encrypted channel and not over unsecured public Wi-Fi or private connection.

7.3 Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.

7.4 Report suspected scams, privacy breaches, and hacking attempts to IT Helpdesk immediately.

8 ADDITIONAL CYBER SECURITY MEASURES

8.1 To reduce the likelihood of security breaches, the following practices are to be adhered to:

- Turn off their screens and lock their devices when leaving their desks;
- Report lost, stolen, or damaged equipment as soon as possible;
- Change all account passwords at once when a device is lost;
- Report a perceived threat or possible security weakness in company systems;
- Do NOT download suspicious, unauthorized or illegal software on their company equipment;
- Do NOT access suspicious websites.

9 HANDLING OF SECURITY INCIDENT

9.1 In the event where a security incident is detected or suspected, e.g. your virus scanning software alerts you that your computer has been infected with malware, you should follow these steps:

- Keep calm and report the incident to IT Helpdesk via phone and not infected device. Using the infected device may spread the damage to other devices;
- Disconnect your computer from the network or internet, and stop and further work with the infected device;
- Determine the type of problem and extent of the impact on your system. Try to identify the source or cause of the problem, such as the opening of a suspicious email;
- Take notes: log down events clearly and tidily and write down the facts, e.g. date and time the incident occurred, what actually happened, who is related to the incident, etc;
- Contain the problem: conduct an impact assessment of the incident and determine any damage or infected data. Move critical data to other media which are separate from the compromised system or network. Shut down or isolate the compromised host temporarily to prevent further damage to other interconnected systems.

--- **END OF DOCUMENT** ---