# Acceptable Use Policy (AUP)

Version 4.1

As at 1 Sep 2016

## 1.0 Purpose

The purpose of this policy is to govern the appropriate use of the organization's IT resources in an effective, secured and lawful manner. As a user, you are responsible for the appropriate use of these IT resources and the safe protection of data.

## 2.0 Scope

This policy applies to all users of the organization's IT resources and data.

Users include (but are not limited to) the organization's employees, contract and temporary staff, contractors, consultants, vendors, and agents (hereafter referred to as 'users') who have been granted access to the organization's IT resources and data.

The organization's IT resources are defined as all the organization's owned, leased, managed, operated, licensed and issued IT hardware, software and services.

The organization's data (hereafter referred to as 'data') is data related to the organization's business activities, that are created, stored, maintained, received and transmitted in electronic and physical form.

Personal devices such as laptops, smartphones, PCs and tablets connected (wired or wireless) locally or remotely to the corporate network for work purposes, or used for storing, transmitting or processing work-related data is subject to this policy.

## 3.0 Use of Organization's IT Resources

The use of organization's IT resources should be work-related and not for personal convenience.

### 3.1 User IDs and Passwords

3.1.1 Users must use strong and unique passwords on their user accounts and comply with the organization's IT security measures such as the regular changing of passwords.

3.1.2 Users must not reveal, share or allow anyone else to use their user ID/token and password on any of the organization's IT resources.

3.1.3 Users must not use someone else's user ID and password to access the organization's IT resources and data.

3.1.4 Users must not leave their user accounts logged in at an unattended and unlocked IT resource.

3.1.5 Users are responsible to inform[1] the organization's IT of the effective date when the status of their user account has changed due to staff reasons such as change of designation/role, resignation, end of contract, transfers or extended absence[2]. For security reasons, the organization's IT reserves the right to disable inactive[3], expired, duplicate or compromised user accounts and to deny access according to access rights policies without notification.

## 3.2 Use of Corporate Email

3.2.1 Users must not use personal email accounts (i.e. Gmail, Yahoo, Hotmail, etc) for work-related communication.

3.2.2 Users must not use corporate email to harass, impersonate, abuse, threaten, annoy or defame, or transmit harmful or malicious content, unsolicited and unauthorised bulk email, junk mail, spam, or chain letters that may otherwise violate the laws of Singapore.

3.2.3 In the event of resignation, end of contract, or end of employment, users are responsible to notify their work-related correspondents before their account expires. They should route or forward their corporate emails, and un-subscribe from mailing lists/groups and mailboxes. The organization's IT will revoke access on the effective date[4] without notification and will not allow access to protect the user's privacy.

## 3.3 Use of Internet

3.3.1 Users must not download and store non-work related audio, video, music, games or other data onto the organization's IT resources.

3.3.2 Users must not access, download, create, send or receive any data (including images), which the organization considers offensive in any way, including sexually explicit, discriminatory, profanity, obscenities, defamatory or libellous material.

3.3.3 Users must not install unlicensed software or be in receipt of, possession of, transmitting and/or downloading, installing, publishing, distributing or copying any

[1] By raising the necessary requests according to the organization's procedures.
[2] Long leave, unpaid leave, attachment, maternity leave, secondment, medical leave or overseas posting longer than 120 days.
[3] Inactive/dormant accounts are defined as user accounts that have no login activity or transaction for 183 days since the last activity.
[4] As notified by HR as the user's last day of service (LDS)

copyrighted or trademarked software without the written consent of the copyright owner.

3.3.4 Users must not use internet document sharing services[5] for work related usage.

## 3.4 Use of Personal Devices

3.4.1 Users are responsible for the organization's data that they capture, display, store, download, transfer, forward or access on or through their personal devices such as laptops, smartphones, personal computers (PC) and tablets.

3.4.2 Users must ensure that personal devices used for work purposes are protected by measures such as anti-virus, password protection and automatic lock-out when the device is not in use or left inactive.

3.4.3 When using personal devices for work purposes, users are responsible to protect them and the organization's data from loss, damage and theft.

3.4.4 Users must not install, configure, synchronize or connect any personal device to the organization's network or IT systems without approval.

## 3.5 Protection of The Organization's Confidential Data[6]

3.5.1 Users must not display, upload, store, transfer or forward any organization's confidential data to the Internet, personal devices, external systems, servers, portals, websites, blog sites or cloud-based services without approval.

3.5.2 Users must ensure that the organization's confidential data in their care is secure from loss, damage and theft.

3.5.3 Users must properly dispose and not leave the organization's confidential data in electronic or physical form on printers, photocopiers, fax machines, waste bins and other non-secured devices and containers.

[5] "Internet document sharing services" such as Dropbox, Onedrive, GoogleDrive, …etc.

[6] "Confidential Data" is defined as:

a. Personal Data means data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access.
b. Patient Data such as health records, medical history, medications, bills, etc
c. Corporate Data such as financial documents, budgets, strategic planning documents, procurement documents, etc
d. Employee Data such as compensation, benefits, work records, etc
e. Intellectual Property such as source code, design documents, processes documentation, pricing lists, research data, etc
f. Any other data defined as confidential by the organization.

3.5.4 In remote, mobile and out-of-office situations, users must use secured means when handling and transferring the organization's confidential data.

3.5.5 Users must not remove, tamper or disable corporate anti-virus and other corporate software installed on the organization's IT resources.

3.5.6 Users must ensure organisation's confidential data is secured during transfer and storage. For example, use of organisation issued encrypted hard disk drive or thumb drive.

## 4.0 Enforcement

All users will be held accountable for the loss of the organization's confidential data. Non-compliance and violations of this Policy will be investigated, leading to disciplinary actions in accordance with the organization's disciplinary procedures.

Users must also not engage in any activities that will be in violation of National Electronic Health Records (NEHR) System Terms of Use and the laws of Singapore, in particular (but not limited to), the Computer Misuse and Cybersecurity Act (Cap 50A), Copyright Act (Cap 63), Spam Control Act (Cap 311A), Undesirable Publications Act (Cap 338) and the Personal Data Protection Act 2012 as may be amended from time to time.

## 5.0 Changes to Policy

The organization's IT may have to amend this Policy or implement additional policies from time to time in the future. Although the organization's IT will endeavour to inform users of policy changes, users must share the responsibility of staying informed.

The current version of the Policy can be found on the organization's Intranet.