Policy Title	Vendor Acceptable Use of IT Resources
Effective Date	17-Mar-2013

1. POLICY STATEMENT

This policy stipulates StarHub governance and guidance on any *StarHub computing facilities and information resources* that are used, accessed, processed, communicated to, or managed by *vendor(s)*.

> *The term "vendor(s)", shall hereafter identify all non-StarHub employee(s) and all other third-party independent business entities/affiliates that are formally contracted to provide products or services to StarHub. Vendor(s) shall include any third-party vendor(s), outsourced vendor(s), contractor(s) and sub-contractor(s), consultant(s), auditor(s) and other external service provider(s).*

> *The term "StarHub computing facilities and information resources" shall hereafter identify all StarHub information entities, and supporting corporate IT facilities and resources that are recognized as important and valuable to StarHub. It includes all the corporate IT systems and services (e.g. BSS, ERP, CRM, CMS, HRMS etc), the corporate Active Directories, the corporate networks and communication infrastructure, the corporate backend servers and clients workstation, the corporate programs and applications less the Network Engineering systems and application, the emails and corporate email systems, the data and corporate data storage, the information documents, the corporate information storage, and processing media and method, the processes and practices, and any information assets, regardless of whether they are owned, loaned, issued, or developed by StarHub, vendor(s) or personal.*

All *vendor(s)* accessing StarHub *computing facilities and information resources*, regardless of whether they are owned, loaned, issued, or developed by StarHub, *vendor(s)* or personal; shall abide to this policy

1.1. Objective

1.1.1. The objective of this policy is to outline the acceptable use, access or management of *StarHub computing facilities and information resources* by *vendor(s)*.

1.1.2. This policy is to serve as a consistent reference for *vendor(s)* to observe good security practice when using, accessing and managing *StarHub computing facilities and information resources.*

1.2. Scope

1.2.1. This policy shall cover the accountability and responsibility of the *vendor(s)* and their respective *StarHub Vendor-in-charge (VIC)* on the acceptable use, access and management of any StarHub *computing facilities and information resource*, including the underlying transacting information/data between StarHub and *vendor(s).*

1.2.2. This policy shall apply to all *vendor(s)*, as well as any StarHub or non-StarHub personnel affiliated with the *vendor(s)*, who are granted on-premise or remote access to *StarHub computing facilities and information resources*, regardless of whether they are using StarHub or non-StarHub computing facilities or workstations.

1.2.3. This policy shall serve in conjunction with all other StarHub policies and standards, particularly those that are *vendor(s)*-related, sets forth in pursuant of information security in StarHub.

1.3. Responsibility and Deviation

1.3.1. Compliance to this policy shall be mandatory.

1.3.2. All StarHub employee(s) and *vendor(s)* shall read this policy document, understand the expectation and take personal responsibility in adherence to the terms and clause herein.

1.3.3. *StarHub VIC* shall ensure that their *vendor(s)* read, understand and comply with the term and clauses herein, and shall be accountable for any of their vendor(s) action.

1.3.4. *Vendor(s)* shall understand that any security violations or misuse of *StarHub computing facilities and information resources* may lead to investigation and initiation of legal or disciplinary actions. StarHub shall reserves all rights to take any action as deemed fit, against the relevant *vendor(s)* who breaches any of the terms and clauses herein.

1.3.5. Deviations from this policy may be justifiable due to business needs, operation constraints, technical feasibility, cost considerations and etc. In the event that any policy clause is deemed inappropriate for application or implementation, the deviation shall be raise and submitted to IS Information Security Manager for approval.

1.3.6. *Vendor(s)* and their respective *StarHub VIC* shall acknowledge their accountability and responsibility by signing off the ***"Declaration for Vendor Acceptable Use of StarHub IT Resources"***, as detailed in ***Appendix A***, before they are allowed access to any *StarHub computing facilities and information resources*.

2. ACCESS CONTROL

2.1. *Vendor(s)* shall NOT access or attempt to access any *StarHub computing facilities and information resources* that they are NOT authorized.

2.2. *Vendor(s)* shall ONLY be granted access to *StarHub computing facilities and information resources* for official purpose and on "need to use" basis.

2.3. *Vendor(s)* shall NOT be granted access to any production or mission-critical system(s), unless authorized and approved by StarHub IS Information Security Manager, with supporting documents (e.g. contract agreement, risk acceptance form etc).

2.4. *Vendor(s)* shall be accountable and responsible for any StarHub access issued to, or under custody of *vendor(s).*

2.5. Where feasible or applicable, *vendor(s)* shall ensure authentication to all *StarHub computing facilities and information resources*.

2.6. Where feasible or applicable, *vendor(s)* shall enable and maintain the access logs, transaction records and audit trails.

2.7. *Vendor(s)* shall take note that all access issue to or under their custody, shall have a maximum validity of 6 months, unless authorized by StarHub IS Information Security Manager, with supporting documents; after which a separate request is required.

2.8. *Vendor(s)* shall surrender all StarHub access at the end of their tenure. *Vendor(s)* shall take concerted effort to remind their respective *StarHub VIC* to terminate their access.

2.9. In the event that *vendor(s)* recognize or suspect that there is a breach in any access controls to *StarHub computing facilities and information resources*, *vendor(s)* shall report the incident to StarHub IS Service Desk or their respective *StarHub VIC* immediately, as stipulated in the ***"Incident Management"*** section of this policy document.

3. ACCOUNT AND PASSWORD MANAGEMENT

3.1. *Vendor(s)* shall be accountable and responsible for any StarHub account(s) and password(s) issued to them or under their custody.

3.2. *Vendor(s)* shall NOT share or reveal any account(s) and password(s) to anyone, including peers, superiors or any StarHub personnel.

3.3. *Vendor(s)* shall NOT write down any account(s) and password(s).

3.4. *Vendor(s)* shall NOT share or reveal any password(s) over the phone.

3.5. *Vendor(s)* shall NOT share or reveal any password(s) that can be identifiable to the associate login credentials, over any forms of electronic communication (e.g. emails, mobile messaging, instant messaging, SMS etc).

3.6. *Vendor(s)* shall NOT store password(s) in clear text or any easily reversible form(s) (i.e. without encryption) in any computer systems, programs, applications, mobile handheld devices etc.

3.7. *Vendor(s)* shall NOT code password(s) in clear text, into applications, programs and data.

3.8. Where feasible or applicable, *vendor(s)* shall abide to the following password management practice:

(a) Enforce password protection.

(b) Disallow blank password.

(c) Change initial/default password(s) upon first login.

(d) Adopt strong password of at least 8 alphanumeric characters in length.

(e) Avoid password(s) that are "easy-to-guess".

(f) Activate screen lock, timeout or logout session during period of inactivity or when not in use; after which a login password must be re-entered to gain access.

(g) Maintain the logs and records of successful and failed login attempts, and any account password changes.

3.9. *Vendor(s)* shall surrender all StarHub account(s) and password(s) issued to them or under their custody, at the end of their tenure. *Vendor(s)* shall take concerted effort to remind their respective *StarHub VIC* to terminate their account(s) and password(s).

2.10. In the event that *vendor(s)* realize or suspect that any of StarHub or StarHub-affiliated account(s) or password(s) have been compromised; *vendor(s)* shall change the password and terminate the connection immediately, and report the incident to StarHub IS Service Desk or their respective *StarHub VIC* immediately, as stipulated in the ***"Incident Management"*** section of this policy document.

4. INFORMATION USAGE AND CONTROL

4.1. *Vendor(s)* shall be responsible and accountable for any StarHub information/data in their possession or custody.

4.2. Any information/data made available to, or obtained by *vendor(s)* shall be classified as confidential unless the information/data is common knowledge in the public domain.

4.3. *Vendor(s)* shall NOT be allowed to share or disclose any confidential information/data without prior approval from the organization.

4.4. *Vendor(s)* shall ensure that any confidential information/data shall be protected against unauthorized access regardless of where it is store; this shall include workstations, notebooks, computer systems, applications, databases, portable storage media, cloud storage, transaction records, temporary transfer directories etc.

4.5. *Vendor(s)* shall NOT use *StarHub computing facilities and information resources* to display, disseminate, or in any way make the information available, if such information is:

(a) Of indecency, seditious, scurrilous, threatening or offensive character or would cause feelings.

(b) Of enmity, hatred, ill-will or hostility between persons of different religious beliefs or faith, different sexes and different races.

(c) Of fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory, or which incite religious or racial intolerance or are otherwise deemed inappropriate.

(d) Likely to cause or which ought to know would cause irritation, annoyance, embarrassment, harassment or nuisance of any kind to other users of the facilities.

(e) Likely to embarrass or bring disrepute to, or which ought to know would embarrass or bring disrepute to StarHub or that of other organizations.

4.6. Vendor(s) shall NOT, under any circumstances and in any manner, transfer or copy any software, computer program, or confidential information/data that is the subject of any copyright, licensing or other intellectual property right from StarHub premises or any *StarHub computing facilities and information resources* without prior approval from the organization.

4.7. *Vendor(s)* shall surrender all StarHub information/data in their custody, at the end of their tenure. *Vendor(s)* shall take concerted effort to remind their respective *StarHub VIC* to takeover these StarHub information/data.

4.8. In the event that *vendor(s)* recognize or suspect that there is a breach in the usage, access, and handing of confidential information/data, *vendor(s)* shall report the incident to StarHub IS Service Desk or their respective *StarHub VIC* immediately, as stipulated in the ***"Incident Management"*** section of this policy document.

5. CORPORATE NETWORK ACCESS AND USAGE

5.1. StarHub corporate network (i.e. LAN and Wireless) shall ONLY be used for official purpose. Any unofficial purpose (e.g. personal, gaming, entertainment, blogging etc) is strictly NOT allowed.

5.2. ONLY Guest Wireless (i.e. Wireless@Green) is opened for public usage.

5.3. Except for the Guest Wireless, *vendor(s)* shall abide to the following practice while using corporate network:

(a) Access and usage shall ONLY be granted on "need to use" basis, subjected to approval by StarHub IS Information Security Manager.

(b) *Vendor(s)* shall NOT connect, install, modify, remove or replace any computer systems, network devices, or any IT gadget (e.g. routers, switches, modems, access points, mobile dongles, PCs, notebooks, printers etc) into the corporate network, unless authorized and approved by StarHub IS Information Security Manager.

(c) *Vendor(s)* shall NOT connect or attempt connections to more than one network at the same time.

5.4. *Vendor(s)* shall NOT engage or attempt to engage in any of the following activities, regardless of whether deliberate or otherwise:

(a) Disrupt any network connectivity and access capability to any *StarHub computing facilities and information resources*

(b) Probe, exploit and circumvent security holes in the corporate network, or that of other organization.

(c) Attack, degrade and damage the performance of the corporate networks, or that of other organizations

(d) Introduces malicious activities and programs into the corporate networks.

5.5. *Vendor(s)* shall take concerted effort to remind their respective *StarHub VIC* to terminate their corporate network access at the end of the tenure.

5.6. In the event that *vendor(s)* recognize or suspect that there is a breach in StarHub corporate network; *vendor(s)* shall report the incident to StarHub IS Service Desk or their respective *StarHub VIC* immediately, as stipulated in the ***"Incident Management***" section in this policy document.

6. INTERNET AND INTRANET ACCESS

6.1. Internet and Intranet access shall ONLY be allowed for official purposes.

6.2. Intranet access shall ONLY be granted to *vendor(s)* on "need to use" basis, subjected to approval by StarHub IS Information Security Manager.

6.3. *Vendor(s)* who have been granted Internet or Intranet access, shall NOT engage in any of the following activities, regardless of whether deliberate or otherwise:

(a) View, store, download, forward or communicate or download any materials that are fraudulent, harassing, embarrassing, sexually explicit, obscene, intimidating, defamatory, or which incite religious or racial intolerance or are otherwise deemed inappropriate.

(b) Upload or post StarHub copyright materials, software or intellectual property to the Internet or Intranet.

(c) Contribute to any online publications and social media such as internet newsgroups, forums, chats, online journals, blogs, tweets podcasts, and etc without being authorized to do so.

(d) Download, install or use any unauthorized or unlicensed software, and any copyright material.

(e) Download or propagate malware (e.g. virus, worms, trojans, botnets etc).

(f) Perform any malicious hacking activities (e.g. network enumeration, vulnerability scanning, identity spoofing, security exploitation, unauthorized access, spamming, denial-of-service and etc).

6.4. *Vendor(s)* shall NOT connect or use any peer-to-peer (P2P) applications, network or resources (e.g. BitTorrent, uTorrent, Gnutella, eDonkey, FrostWire etc).

6.5. *Vendor(s)* shall take concerted effort to remind their respective *StarHub VIC* to terminate their Intranet access at the end of the tenure.

6.6. In the event that *vendor(s)* recognize or suspect that there is a breach from their Internet, access or compromised in their Intranet access; *vendor(s)* shall report the incident to StarHub IS Service Desk or their respective *StarHub VIC* immediately, as stipulated in the ***"Incident Management"*** section of this policy document.

7. EMAIL SERVICE AND USAGE

7.1. Email services shall ONLY be allowed for official purposes, and granted to *vendor(s)* on "need to use" basis, subjected to approval by IS Information Security Manager

7.2. *Vendor(s)* who have been granted email services shall NOT engage in any of the following activities, regardless of whether deliberate or otherwise:

(a) Send and/or knowingly receive email that is fraudulent, obscene, racist, harassing, intimidating or otherwise offensive, harmful or prejudicial to the interest of StarHub;

(b) Use email for commercial solicitation, distribution of hoaxes, chain letters, advertisements or any personal matters;

(c) Introduce or propagate malware (e.g. virus, worms, trojans, botnets etc).

(d) Engage in any form of mail spoofing, including attempting to send mail such that its origin appears to be from another user or machine, or a non-existent machine.

(e) Engage in any form of mail spamming which may prevent the recipient from accessing his/her mailbox or adversely affect the organization's email servers.

(f) Send, forward and/or reply to large list of recipients concerning unofficial matters.

7.3. *Vendor(s)* shall surrender all StarHub email access issued to them or under their custody, at the end of their tenure. *Vendor(s)* shall take concerted effort to remind their respective *StarHub VIC* to terminate their email access.

7.4. In the event that *vendor(s)* recognize or suspect that their email have been spoofed, spammed or compromised; *vendor(s)* shall report the incident to StarHub IS Service Desk or their respective *StarHub VIC* immediately, as stipulated in the ***"Incident Management"*** section of this policy document.

8. MALICIOUS ACTIVITIES AND MALWARE PREVENTION

8.1. *Vendor(s)* shall NOT circumvent the security of any *StarHub computing facilities and information resources*.

8.2. *Vendor(s)* shall NOT perform any malicious activities, or introduce any malware programs, regardless of whether deliberate of otherwise (e.g. network enumeration, vulnerability scanning, identity spoofing, email spamming, security exploitation, session hijacking, unauthorized access, denial-of-service etc)

8.3. *Vendor(s)* shall NOT install or use any applications that may cause disrupt, damage, exploit and/or circumvent the security of StarHub *computing facilities* or *information resources;* regardless of whether deliberate or otherwise (e.g. network analyzer, host/port scanners, password crackers, key loggers, key generators etc)

8.4. Where technically feasible, *vendor(s)* shall abide to the following malware prevention practice; regardless of whether their *computing facilities* are loaned, issued or owned by StarHub, *vendor(s)* or personal:

(a) Ensure that antivirus software and personal firewall are installed, enabled at all times and kept up-to-date with the latest patch and virus definition.

(b) Schedule for a full system virus scan on weekly basis.

(c) Perform full system virus scan before connecting to StarHub corporate network for the first time.

(d) Perform virus scan to any files that are being used for the first time before connecting to StarHub corporate network

(e) Disconnect from StarHub corporate network immediately if it is infected, or suspected to be infected, by malware; can ONLY be re-connected to after the malware has been successfully eradicated.

8.5. *Vendor(s)* shall ensure that any storage media (e.g. portable harddisk, thumb drive, CDs, DVDs etc) that is infected or suspected to be infected by malware, shall NOT be used in any StarHub *computing facilities*, until the virus in the storage media has been successfully eradicated.

8.6. In the event that *vendor(s)* recognize or suspect that there is malware propagation, or any malicious attempts or tampering to *StarHub computing facilities and information resources*; *vendor(s)* shall report the incident to StarHub IS Service Desk or their respective *StarHub VIC* immediately, as stipulated in the ***"Incident Management"*** section of this policy document.

9. PHYSICAL SECURITY

9.1. *Vendor(s)* shall ensure that all portable *computing facilities* are securely locked away when not in use, or secured with quality cable locks where applicable. This includes notebooks, portable storage media, security tokens, mobile devices etc, regardless of whether they are loaned, issued or owned by StarHub, *vendor(s)* or personal.

9.2. *Vendor(s)* shall ensure that screen saver, screen lock, timeout or logout session are enabled where applicable, for period of inactivity or when not in use; after which a login password must be re-entered to gain access.

9.3. *Vendor(s)* shall NOT leave that any StarHub information/data unattended at all times, regardless of whether they are hardcopy document or softcopy media. all StarHub information/data (in any form) shall be securely locked away when not in use or required.

9.4. *Vendor(s)* shall remove documents from the printers and/or facsimiles immediately.

9.5. *Vendor(s)* shall ensure that any unwanted information/data, regardless of whether they are softcopy or hardcopy, are properly discarded are disposed (e.g. shredding of hardcopy, degaussing of storage etc).

9.6. *Vendor(s)* shall visibly display their security pass at all times when they are in StarHub premises; these security pass shall be returned at the end of their tenure, or when they are leaving StarHub premises, whichever relevant.

9.7. In the event that *vendor(s)* recognize or suspect that there is physical security breach to any *StarHub computing facilities and information resources*, *vendor(s)* shall report the incident to StarHub IS Service Desk or their *StarHub VIC* immediately, as stipulated in the ***"Incident Management"*** section of this policy document.

10. REMOTE ACCESS

10.1. Remote access into any *StarHub computing facilities and information resources* shall ONLY be allowed for official purposes, and be granted to *vendor(s)* "need to use" basis, subjected to approval by IS Information Security Manager.

10.2. *Vendor(s)* shall be aware of their responsibilities when accessing *StarHub computing facilities and information resources* outside StarHub premises, where the risk of security exposure are higher.

10.3. *Vendor(s)* shall disconnect all remote connections, when not in use.

10.4. *Vendor(s)* shall take concerted effort to remind their respective *StarHub VIC* to terminate their remote access at the end of the tenure.

10.5. *Vendor(s)* shall adhere and abide to the all the terms and clauses as stipulated in this policy document, regardless of whether they are accessing from within StarHub premised, or any remote site outside of StarHub premises.

10.6. In the event that *vendor(s)* recognize or suspect that there is a breach to their remote access to any *StarHub computing facilities and information resources*, *vendor(s)* shall report the incident to StarHub IS Service Desk or their respective *StarHub VIC* immediately, as stipulated in the ***"Incident Management"*** section of this policy document.

11. SECURITY TOKEN USAGE

11.1. Security Token(s) may be issued for *2nd Factor Authentication (2FA)*; typically to facilitate *vendor(s)* to authenticate remotely into *StarHub computing facilities and information resources*.

11.2. *Vendor(s)* shall ONLY use the Security Token(s) according to the purpose for which they are provided.

11.3. Security Token(s) are governed with PINs. *Vendor(s)* shall safeguard the use and handling of the Security Token PIN in similar manner as stipulated in the ***"Accounts and Password Management"*** section of this policy document

11.4. Should there be a need to change the Security Token PIN, *vendor(s)* shall contact the StarHub IS Service Desk or their respective *StarHub VIC* to facilitate the request.

11.5. *Vendor(s)* shall take proper care of the Security Token(s) issued to them or under their custody; failing which, a SGD $120.00 fine will be imposed as cost of replacing a lost or damaged token.

11.6. *Vendor(s)* shall surrender any Security Token(s) issued to them or under their custody at the end of their tenure. *Vendor(s)* shall take concerted effort to remind their respective StarHub Vendor-in-charge to collect Security Token(s) from them and return the Security Token(s) to StarHub IS Information Security Team.

11.7. In the event that *vendor(s)* lose, misplace or damage their Security Token, or realize or suspect that the Security Token has been stolen or tampered, or the PIN has been compromised; *vendor(s)* shall report the incident to StarHub IS Service Desk or their respective *StarHub VIC* immediately, as stipulated in the ***"Incident Management"*** section of this policy document, to deactivate the Security Token, and for subsequent replacement.

12. INCIDENT MANAGEMENT

12.1. *Vendor(s)* shall report all IT security incidents to their respective *StarHub VIC*.

12.2. *Vendor(s)* shall report immediately any damaged, misplaced, lost or stolen *StarHub computing facilities and information resources* to respective *StarHub VIC*.

12.3. *StarHub VIC* shall report all IT security incident reported by *vendor(s)* to StarHub IS Service Desk. *Vendor(s)* shall take concerted effort to ensure that the IT security incident is relayed by their respective *StarHub VIC*.

12.4. *Vendor (s)* shall NOT try to solve any IT security incidents by themselves unless guided by StarHub IS Service Desk or IS Information Security personnel.

12.5. *Vendor(s)* shall provide any information required or requested by the StarHub IS Service Desk or IS Information Security personnel to help in investigations.

13. WORKSTATION USAGE

13.1. Any usage of workstation(s) by *vendor(s)* to access *StarHub computing facilities and information resources* shall ONLY be allowed for official purpose, and granted on "need to use" basis.

13.2. Any workstation(s) made available to, used by, obtained by, or under the custody of *Vendors(s)*; regardless of whether StarHub or non-StarHub, shall be classified as *vendor workstation(s).*

> *"Vendor workstation(s)" shall hereafter include all StarHub and non-StarHub PCs, notebooks and any computer work terminals; regardless of whether they are owned by, loaned by, used by, issued to, or under the custody of vendor(s)*

13.3. Where technically feasible, all *vendor workstation(s)* shall abide to the following malware prevention practice:

(a) Installed, and enabled with antivirus software and personal firewall software

(b) Kept up-to-date with the latest system, security and applications patches before they can be used to access any StarHub *computing facilities and information resources*.

(c) Activate screen lock, timeout or logout session during period of inactivity or when not in use; after which a login password must be re-entered to gain access

(d) Maintain logs and records of access and transactions.

13.4. *Vendor(s)* shall adhere and abide to the terms and clauses as stipulated in this policy document, in pursuant to safeguard the use, access and management of the *vendor workstation*(s).

StarHub Workstation

13.5. *StarHub workstation(s)* shall ONLY be used by, issued to, or assigned under the custody of *vendor(s)* for official purpose on "need to use" basis.

13.6. *Vendor(s)* shall ONLY use the *StarHub workstation(s)* according to the purpose for which they are provided

13.7. *Vendor(s)* shall be accountable and responsible for the *StarHub workstation(s)* assigned to them or under their custody.

13.8. *Vendor(s)* using *StarHub workstation(s)* shall NOT be granted "Administrator" rights, unless authorized and approved by StarHub IS Information Security Manager.

13.9. "Administrator" rights for *StarHub workstation(s)* are granted on "need to use" basis.

13.10. *Vendor(s)* using *StarHub workstation(s)* shall NOT modify or attempt to modify any settings, configurations, or make any hardware and software changes to the workstation that may pose security threats, or risk to the workstation or to any StarHub *computing facilities and information resources*.

13.11. *Vendor(s)* using *StarHub workstation(s)* shall NOT install and use or install unauthorized and unlicensed software. ONLY ***authorized software*** and applications shall be allowed to be installed in *StarHub workstation*

> *"Authorized software" shall hereafter referred to software that (a) licensed and used in accordance with the software licensing agreements, (b) legally acquired, and (c) approved by StarHub.*

13.12. *Vendor(s)* shall NOT transfer any software or application license key(s) already installed in one workstation to another.

13.13. *Vendor(s)* shall NOT circumvent the security of the *StarHub workstation*.

Non-StarHub Workstation

13.14. Any usage of non-StarHub workstation to use or access *StarHub computing facilities and information resources* shall be granted on "need to use" basis.

13.15. *Vendor(s)* shall NOT connect any *non-StarHub workstation*s to StarHub corporate network, unless being authorized and approved by StarHub IS Information Security Manager

13.16. All information/data stored in, or processed from *non-StarHub workstation*(s) shall be the property of StarHub, accountable and responsible by the *vendor(s).*

13.17. *Vendor(s)* shall be aware of their responsibilities when using *non-StarHub workstation* to use, access or manage *StarHub computing facilities and information resources*.

13.18. *Vendor(s)* shall NOT transfer any software or application license key(s) from a StarHub workstation to a *non-StarHub workstation* and vice versa.

13.19. *Vendors* who are using *non-StarHub workstation(s)* shall declare and provide details of their workstation as required in the "***Declaration for Vendor Acceptable Use of StarHub IT Resources"*** as stipulated in ***Appendix A*** of this policy document.

14. VERSION HISTORY

Version	Responsible	Change Description	Date
1.0	Joshua Yip	Baseline version	07 Mar 2013

Appendix A: Declaration for Vendor Acceptable Use of StarHub IT Resources

I understand and agree to abide by the terms and clauses as stipulated in this policy on ***"Vendor Acceptable Use of IT Resources"***. I further understand that any violation of the regulations set forth by the policy may constitute a criminal offense and/or subject to legal action, and agree to be jointly and severally liable, with the organization I represent, for any damages, losses, costs and expenses incurred or suffered by StarHub Ltd.

Select the below option if you are using a non-StarHub workstation to access StarHub computing facilities and information resources.

☒ **Yes**, I am using the following non-StarHub workstation to access StarHub corporate resources.

Non-StarHub Workstation Details			
Brand and Model : HP Z230 Workstation		**Serial No** :	
Computer Name : Reggie-14030		**Operating System** : Windows 7 Professional SP 1	
LAN MAC Address : 64-51-06-44-4C-45		**Wireless MAC Address** :	
Please ensure the workstation meets the following requirements by putting a tick on the checkbox.			
☒ Antivirus and Personal Firewall software are installed, enabled and updated with the latest antivirus definition and security patch	☒ Operating System is installed and patched with latest service pack and/or security updates	☒ Software/application program(s) are installed with latest security updates	☒ Software/application that may disrupt, damage, exploit or circumvent the security of StarHub networks and systems are NOT installed *(e.g. network scanners, vulnerability scanners, key loggers, password crackers, software key gens, P2P etc)*

I declare that the information provided in this form is true and complete. My signature below indicates that I have read, understand, and agree to abide by all the terms and clauses stipulated in this policy on ***"Vendor Acceptable Use of IT Resources"***.

Name : Reggie Salido Senal

NRIC/Identification No : G0996085L

Company : Tribal Worldwide Pte Ltd

Period of Access* (dd/mm/yy) : From 01/01/18 To 31/12/17

Signature : 

Date Signed : 22/11/16

TO BE COMPLETED BY STARHUB VENDOR-IN-CHARGE

As the StarHub Vendor-in-charge of the personnel listed above, I have read, understand and agree to abide by the terms and clauses stipulated in this policy for ***"Vendor Acceptable Use of IT Resources"***. I have reviewed and verified the content of the form is true to the best of my knowledge. I am fully aware of this request and any possible risks that accompanies, with vendor using or accessing StarHub computing facilities and information resources. I shall hereby acknowledge my responsibility to ensure that vendor complies with the term and clauses herein and shall be accountable for any of their action.

Name : Priscilla Quek

Email Address : lmquek@starhub.com

Mobile No : 9656 9956

Business Unit (Dept/Section/Team) : CBG / Integrated Marketing / Digital

Signature :

Date Signed : 22/11/16

All vendor access will have a maximum validity of 6 months; after which a separate request is required if extension is needed