Triple H Cloud Services (Pty) Ltd (THCS)

Acceptable Usage Policy

REVIEW SCHEDULE

Date created or reviewed	Version number	Review notes	Person who reviewed
July 2019	V1.00	This document was created in July 2019	Kent Hutchons

TABLE OF CONTENTS

1. Purpose

This acceptable usage policy clearly indicates what information system users are and are not allowed to do. The potential exists that, without this policy, information system users could violate information security and avoid punitive actions by claiming to not know about any restrictions in place. This can make it extremely difficult to enforce the measures outlined in the policy and ultimately lead to a complete disregard of the policy.

2. Scope

This Acceptable Usage Policy applies to all users of all information systems that are the property of Triple H Cloud Services (Pty) Ltd (hereafter referred to as THCS).

Specifically, it includes:

- All employees, whether employed on a full-time or part-time basis by THCS.
- All contractors and third parties that work on behalf of and are paid directly by THCS.
- All contractors and third parties that work on behalf of THCS but are paid directly by an alternate employer.
- All employees of partners and clients of THCS that access THCS's non-public information systems.

3. Policy

THCS will issue acceptable usage guidelines covering the following items:

3.1 Computer and information system usage
3.2 Software and data usage
3.3 Internet and e-mail usage
3.4 Newsgroups
3.5 Telephone usage
3.6 Office equipment & materials usage
3.7 Privacy and Confidentiality
3.8 Social media usage
3.9 IT Security Do's and Don'ts

As a requirement of information system access, and as a component of security awareness training, all information system users, whether employees or third parties, will be required to provide signed acceptance of the acceptable usage guidelines. A copy of the signed document will be provided to the individual with the original being retained by the appropriate Human Resources department.

Presenting the access to information resources is a combined effort that requires each employee to act responsibly and to guard against abuse. Therefore, each individual user has an obligation to abide by the following standards of acceptable and ethical use as described in the policy document:

- Protect the access and integrity of computing and information technology resources;
- Abide by applicable laws and respect the copyright and intellectual property rights of others, including the legal use of licensed software;
- Respect the privacy and personal rights of others; and
- THCS sensitive information must not be forwarded to any party outside THCS without prior approval from the THCS IT Director.

3.1 Computer and information system usage

Systems, including computers and other related technology, are the property of THCS.

Access to, and use of, systems and the components that form them will be monitored and controlled at all times.

Presenting the access to information resources is a combined effort that requires each employee to act responsibly and to guard against abuse. Therefore, each individual user has an obligation to abide by the following standards of acceptable and ethical use as described in this policy document;

- Accessing computers, computer software, computer data or information, or networks without proper authorisation, regardless of whether THCS owns the computer, software, data, information, or network in question;
- Transmitting on or through any of THCS's systems, services, or products any material that is unlawful, obscene, racial, pornographic, threatening, abusive, libelous, or hateful, is or encourages conduct that may constitute a criminal offence, may give rise

to civil or any other liability, or otherwise may violate any local, state, national or international law.

- Consuming excessive resources, including CPU time, memory, disk space, and session time for personal use, is prohibited. The use of resources-intensive programs, which negatively affect other system users, or the performance of THCS's systems or networks.
- Intercepting or examining the content of messages or files in transit on a network without authorisation from the owner of the information, or when it is not specifically part of the job function to perform such an action.

3.2 Software and data usage

The software tools the organisation provides and the data they create and manipulate are the property of THCS:

- Software is to be used for its intended purpose only. It is not to be copied, distributed, installed, or deleted without appropriate authorisation. Such activities will be monitored and controlled at all times.
- Data is to be used for its intended purpose. It is not to be copied, distributed, edited, appended, or deleted without appropriate authorisation. Such activities will be monitored and controlled at all times.
- Violating any software license agreement or copyright, including copying or redistributing copyrighted software, data, or reports without proper, recorded authorisation, is prohibited.
- Violating the property rights or copyrights of software holders or the holders of computer generated data or reports without proper, recorded authorisation, is prohibited.

3.3 Internet and e-mail usage

Internet and e-mail usage must be restricted as both activities make use of public and unsecured networks:

- The Internet is to be used for business purposes and usage will always be monitored and controlled;
- E-mail is to be used for business purposes only and usage will always be monitored and controlled;

- Affecting security breaches or disruptions of Internet communications is prohibited. Security breaches include but are not limited to; accessing data not intended for the recipient or logging onto a server or account, that the user is not expressly authorised to access by whatever means. For purposes of this section, “disruption” includes, but is not limited to; port scans, ping floods, packet spoofing, forged routing information, deliberate attempts to overload a service, attempts to “crash” a host, and the introduction of any malicious code, such as computer viruses or “trojans”, onto any part of THCS’s computer network.

- Email:
  - *Intimidation*

    It is a violation of this policy to send electronic mail that is abusive or threatens an individual’s safety. The use of electronic mail for sexual, ethnic, religious, or any other harassment is also prohibited. Threats to personal safety should be reported to the appropriate line manager.

  - *Harassment*

    It is a violation of this policy to use electronic mail to harass an individual. This includes sending or forwarding chain letters, deliberately flooding a user’s mailbox with automatically generated mail that is designed to interfere with proper mail delivery or access.

  - *Unsolicited Mail*

    Sending unsolicited mail messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (“e-mail spam”) is prohibited. It is explicitly prohibited to send unsolicited bulk mail messages. If a recipient asks to stop receiving e-mail, then the user must not send that person any further e-mail. This does not apply to normal business information messages.

- *Chain Letters*

  Creating or forwarding “chain letters” or other “pyramid schemes” of any type, whether or not the recipient wishes to receive such mailings.

- *Malicious E-Mail*

  Malicious e-mail including, but not limited to ”mail bombing” (flooding a user or site with very large or numerous pieces of e-mail).

- *Forged Mail*

  It is a violation of this policy to forge an electronic mail signature to make it appear as though it originated from a different person, whether through unauthorised use, or forging, or mail header information alteration or otherwise. This does not apply to normal business practice where an assistant or secretary replies on behalf of someone else.

- *Unauthorised Collection of Mail*

  It is a violation of this policy to use a company or a client account to collect replies to messages sent from another provider.

- *Unauthorised Access*

  It is a violation of this policy to attempt to gain access to another person’s mail files regardless of whether the access was successful or whether or not the messages accessed involved personal information.

- *Copyrighted Material*

  It is a violation of this policy to send unauthorised copyrighted materials electronically.

- *Username Dissemination*

  A person's username and e-mail address are considered public information that can be given out to other individuals. No one will knowingly permit its release for the purpose of advertising, mass mailings, or other commercial uses without the permission of the individual.

- *Termination of Service*

  Users whose service with THCS has been terminated will have no rights of access to the contents of messages addressed to them whether official or private.

3.4 Newsgroups

The following serves as a guideline towards what THCS considers being the misuse of computing resources and privileges. These actions are prohibited except when the employee is authorised to do so as part of the normal job function.

- Posting the same or similar messages to large numbers of Newsgroups ("Newsgroup spam or USENET spam").
- Posting chain letters of any type.
- Posting encoded binary files to newsgroups not specifically named for that purpose.
- Cancellation or superseding of posts other than own posts, with the exception of official newsgroup moderators performing their duties.
- Forging of header information is prohibited. This includes the circumvention of the approval process for posting to a moderated newsgroup.
- Solicitation of mail for any other e-mail address other than that of the poster's account or service, with intent to harass or to collect replies.
- Posting of articles from the THCS network or networks of other Internet Service providers on behalf of, or to advertise any service hosted by THCS, or connected via the THCS network without written permission from management.

3.5 Telephone usage

The telephone system, including all telephones and fax machines, is the property of the organisation:

- The telephone system, including all and analog and digital lines, is to be used for business purposes only and may be monitored and will be controlled at all times.

3.6 Office equipment and materials usage

The office materials, furnishings and supplies provided to employees are the property of the organization and are to be used for business purposes only:

- Generic materials (those that do not imply consent of the organization such as pens, blank paper, etc.) may be freely accessed but are not to be removed from those facilities without prior consent.
- Specific materials (those that imply consent of the organization such as letterhead and stamps, etc.) must have restricted access and are not to be removed from the facilities without prior consent.
- Individuals shall not place any THCS material (software, internal memos etc) on any publicly accessible internal or external website without prior approval from the Chief Executive Officer

3.7 Privacy and confidentiality:

- Transmission, distribution, or storage of any information, data or material in violation of laws or regulations, including the common law.
- Violation of the rights of any person, protected by the law regarding copyright, trade secret, patent or other intellectual property or similar rights, laws or regulations.
- Actions that restrict or inhibit any person, whether a user of THCS or otherwise, in his use of enjoyment of any of THCS's systems, services or products

3.8 Social Media usage

The organization's social media accounts are intended to be used solely for business purposes. Depending on the nature of the employee's duties, these purposes may be addressed through a variety of services, including but not limited to Facebook, Twitter, LinkedIn, and YouTube.

The following activities are deemed inappropriate uses of social media:

- Use of social media for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
- Use of social media that in any way violates the company's policies, rules, or administrative orders, including, but not limited to, [list any applicable code of conduct policies, etc.].
- Opening attachments from unknown or unsigned sources. Attachments are the primary source of computer viruses and should be treated with utmost caution.
- Sharing social media account passwords with another person or attempting to obtain another person's social media account password.

3.9 IT Security Do's and Don'ts

Do's

- Use only those computing and information technology resources for which authorisation have been given.
- Use computing and information technology resources for their intended purpose.
- Always lock your computer and mobile phone when not in use.
- Stay alert and always report any suspicious activity to IT. If something goes wrong, the faster we know about it and the faster we can deal with it.
- Always password-protect sensitive files on your computer; USB flash drive; smartphone; laptop etc. When losing the device, strong passwords will make it difficult for someone to break in and steal data.
- Always create complex passwords by including different letter cases, numbers, and punctuation. Attempt to use different passwords for different websites and computers.
- When you plug in personal devices such as USB's, MP3 players and smartphones, always ensure that the device is not infected with a virus.
- Be cautious of suspicious emails and links. Always delete suspicious emails and never click on the links.
- Always log off whenever you leave your workstation so no one can perform any activity under their user ID when they are away.

- Exercise caution when forwarding messages as some information that is intended for a specific individual may not be appropriate for general distribution.

Don'ts

- Don't be tricked into giving away confidential information

  E.g. respond to emails or calls requesting confidential company or personal information;
- Don't use an unprotected computer to access THCS's system

  E.g. malicious software exists, if you are unsure the computer you are using is not safe don't use it to access corporate or sensitive data.
- Don't leave sensitive information lying around the office

  E.g. printouts containing private information on your desk.
- Don't install unauthorized programs on your work computer. Malicious applications often pose as legitimate programs e.g. games, tools or even antivirus software.
- Don't furnish false data on any sign-up form, employment contract, or online application, including fraudulent use of credit card numbers (such conduct is ground or reason for immediate termination and may subject the individual to civil or criminal liability).
- Don't misrepresent identity - use an anonymous identity or someone else's identity password or ID address for the purpose of wronging or disadvantaging that person
- Don't attempt to circumvent user authentication or security of any host, network, or account ("cracking"). This includes, but is not limited to, accessing data not intended for the recipient/user, logging into a server or account the user is not expressly authorised to access, or probing the security of other networks (such as running automated security scans or similar tools).
- Loopholes in computer security systems or knowledge of any password, or any other information used for authentication purposes, should not be used to damage computer systems, obtain extra resources, take resources from another user, gain access to systems or use systems for which proper authorisation was not given.
- Don't use any program/script/command, or sending messages of any kind, designed to interfere with user's terminal session, by any means, locally or via the Internet.

- Don’t execute any form of network monitoring which will intercept data not intended for a specific employee’s use.

4. Non-Compliance

Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken:

- A minor breach will result in written reprimand.
- Multiple minor breaches or a major breach will result in suspension.
- Multiple major breaches will result in termination.

5. Policy review and training

The policy will be reviewed, and employees must be trained annually about IT security threats, and as and when there is any change in legislation