Ralco Coporation Berhad

IT Policy

- **PURPOSE**

The purpose is to define the policy and responsibilities necessary to ensure appropriate, efficient and responsible use of computer resources. This policy helps to ensure that computer resources are utilised and used in compliance with applicable laws and software license agreements and outline the acceptable use of computer equipment at Ralco Corporation Bhd and it's subsidiaries (herein refer to as the Group). These rules are in place to protect the Company and it's employee

- **SCOPE**

This policy applies to employees, contractors, consultants, temporaries, and other workers in the Group including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Group. It also applies as to whether access is on-site or from any remote locations.

- **ACRONYMS & DEFINITIONS**

Term	Definition
SPAM	Unauthorized and/or unsolicited electronic mass mailings
Computing Systems	The Group computing systems are computer, peripherals, printers, plotters, scanners, modems, internal and external networks, electronic mail, facsimile devices, paging devices, and other computer devices and systems owned or leased by the Group whether used by employees, agents, partners, or contractors or any other authorized non-Ralco employee

- **POLICY**

1.0 OVERVIEW

1.1 The Group intentions for publishing an Acceptable Use Policy is to protect the Companies and all its employees, partners from illegal or damaging actions by individuals, either knowingly or unknowingly. Our computing systems and environment are to be used soley for business purposes in serving the best interests of the company, and of our clients and customers in the course of normal operations. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, accounts, and net browsing sites designed and owned by the Group, are the property of Ralco Corporation

1.2 Effective security is a team effort involving the participation and support of every employee, contractor, partner, and agency of the Group who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly with integrity.

1.3 The policy statement states the requirement or restriction which this policy is placing on the organization and why. It does not describe “how to” procedures.

2.0 GENERAL USE

2.1 Each user within the Group when utilizing any computer resources shall be aware of the provisions of this policy before being given access to the Group’s computer resources.

2.2 While Group’s network administration desires to provide a reasonable level of privacy, users shall be aware that the data they create on the corporate systems remains the property of Ralco Corporation Bhd. Because of the need to protect the Group’s network, management cannot guarantee the confidentiality of information stored on any network device belonging to the Group

2.3 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees shall be guided by departmental policies on personal use, and if there is any uncertainty, employees may consult their supervisor or manager.

2.4 For security and network maintenance purposes, authorized individuals within the Group may monitor equipment, systems and network traffic at any time. Ralco Corporation Bhd also reserves the right to add necessary files and modify the configuration of any connected computer or system to ensure the security and integrity of its computing resources.

2.5 Ralco Corporation Bhd reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.6 Ralco Corporation Bhd’s computer transactions shall be traceable to the initiating user

3.0 SECURITY AND PROPRIETARY INFORMATION

3.1 The user interface for information contained on Internet/Intranet/Extranet-related systems shall be classified as either general public, internal use only, or confidential, as defined by corporate confidentiality guidelines. Employees shall take all necessary steps to prevent unauthorized access to this information.

3.2 Authorized users are responsible for the security of their accounts and any related authentication devices or credentials, such as passwords, pass-codes, or PINS. They shall ensure authentication devices and credentials are kept secure and shall not share accounts except as permitted by management.

3.3 All PCs, laptops and workstations shall be secured with a password-protected screensaver with the automatic activation feature set at 2 minutes or less, or by logging-off (control-alt-delete for Window users) when the host is unattended.

3.4 Because information contained on portable computers is especially vulnerable, special care shall be exercised. Protect laptops in accordance with the current virus-scanning software.

3.5 Internet/Intranet/Extranet, whether owned by the employee or PCM, shall be continually executing approved virus-scanning software with a current virus database.(Unless overridden and documented by departmental or group policy).

3.6 Employees shall use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code or Malware.

4.0 UNACCEPTABLE USE

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of Group authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Ralco's-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.1 Prohibited System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Group.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Ralco or the end user does not have an active license is strictly prohibited.

- Disclosing confidential information which is owned by or entrusted to the Group to unauthorized recipients is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management shall be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, Malwares,e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Ralco computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction or participating in any activity which could be discriminatory or intimidating to others..
- Using a Ralco computing asset to create, store, view or transmit pornographic material.
- Making fraudulent offers of products, items, or services originating from any Ralco’s account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Communicating in ways that disparage other companies’ products or services.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Executing any form of network monitoring which intercepts data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Removing, interfering with, or preventing the installation of Ralco authorized and managed applications specifically installed to monitor activities and manage compliance of computing devices on the Ralco network such as Microsoft System Management Server and similar software.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Ralco’s employees to parties outside the Company

- Promoting personal political or religious positions to fellow employees at workplace.
- Soliciting on behalf of charitable, commercial, or internal organizations, or otherwise, except as provided by appropriate Ralco HR policies/procedures on solicitation and distribution

4.2 Prohibited Email and Communication Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Ralco 's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Ralco or connected via Ralco's network
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Monitoring another’s email unless specifically authorized by Ralco Human Resources
- Automatically forwarding Ralco electronic communications to non-Ralco accounts in a non-secure fashion. This includes auto-forwarding of an entire E-mail account to an external account (ex. Hotmail, yahoo, msn, Skytel, etc.) Secured messaging transactions to secured devices is permissible as long as the secured forwarding access is controlled and managed exclusively by Ralco.

5.0 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. All authorized non-employee users within the scope of this policy who are found to have violated this policy are subject to sanctions for non-compliance as incorporated into related contracts or agreements.