





MicroVentures Philippines Financing Company Inc.
Unit 2906 One San Miguel Avenue Office Condominium
San Miguel Avenue cor. Shaw Blvd., Bgy. San Antonio
Ortigas Center, Pasig City 1600
Tel No. +63 (2) 2340845
Fax No. +63 (2) 5701979
www.onepuhunan.com.ph

Policy No.	:	INFORMATION SECURITY POLICY 2017 - 01	
Policy Name	:	ACCEPTABLE USE POLICY	
Version No.	:	1.0	
Effectivity Date	:	2017 March 01	
Replaces	:	- n/a -	
Target Group	:	ALL EMPLOYEES	
Total Pages	:	4	
Approved By	:	IT HEAD	 RAMEL E. ROBLES
	:	PRESIDENT	 DANIELE ROVERE

INFORMATION SECURITY POLICY 2017-01

POLICY NAME : ACCEPTABLE USE POLICY

1.0 Overview

MicroVentures Philippines Financing Company Inc. (OnePuhunan)'s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to its established culture of openness, trust and integrity. The Company is committed to protecting its employees, partners and itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of the company. These systems are to be used for business purposes in serving the interests of the company, and of its clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every employee and affiliate who deal with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and systems in the company. These rules are in place to protect the employee and the company. Inappropriate use exposes the company to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, on-the-job trainees, temporaries, and other workers in the company, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the company.

4.0 Policy

General Use and Ownership

- While the company's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the company. Because of the need to protect the company's network, management cannot guarantee the confidentiality of personal information stored on any network device belonging to the company.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor / manager or Information Technology.
- For security and network maintenance purposes, authorized individuals within the company may monitor and record equipment, systems and network (including video, voice, and data) activity/traffic at any time.

- The Company reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

- The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off (control-alt-delete for Windows users) when the host will be unattended.
- Use encryption of information whenever possible during transmission of confidential information over the network.
- Postings by employees using a company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the company, unless posting is in the course of business duties.
- All hosts or devices used by the employee that are connected to the company Internet/Intranet/Extranet, whether owned by the employee or the company, shall be continually executing approved virus-scanning software with a current virus database whenever possible unless overridden by departmental or group policy.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

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 the company authorized to engage in any activity that is illegal under local, national or international law while utilizing company-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.

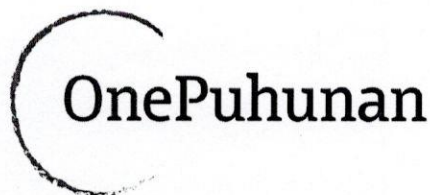
- **System and Network Activities**

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 company.

- 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 the company or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should 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, 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 company 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.
- Making fraudulent offers of products, items, or services originating from any company account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- 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.
- Port scanning or security scanning is expressly prohibited unless prior notification to the company's Information Technology Head is made.
- Executing any form of network monitoring which will intercept 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.
- 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, company employees or customers to parties outside of the company other than those considered as official by the company (ex. SSS, BIR, PhilHealth, CIC).
- **Email and Communications 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) (refer to the company's *Email Policy*).
 - Any form of harassment via email, telephone or forms of messaging.
 - 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", "Ponzi" or other "pyramid" schemes of any type.
 - Use of unsolicited email originating from within the company's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise any service hosted by



MicroVentures Philippines Financing Company Inc.
Unit 2906 One San Miguel Avenue Office Condominium
San Miguel Avenue cor. Shaw Blvd., Bgy. San Antonio
Ortigas Center, Pasig City 1600
Tel No. +63 (2) 2340845
Fax No. +63 (2) 5701979
www.onepuhunan.com.ph

MicroVentures Philippines Financing Company Inc. or connected via the company's network.

- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging

- Blogging by employees, whether using the company's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of the company's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate company policies, is not detrimental to the company's best interests, and does not interfere with an employee's regular work duties. Blogging from the company's systems is also subject to monitoring.
- Employees are prohibited from revealing any MicroVentures Philippines Financing Company Inc. confidential or proprietary information, trade secrets or any other material deemed sensitive by the company when engaged in blogging.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the company and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the company's policy against discrimination and harassment.
- Employees may also not attribute personal statements, opinions or beliefs to the company when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the company. Employees assume any and all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, the company's trademarks, logos and any other company intellectual property may also not be used in connection with any blogging activity.

5.0 Enforcement

Any employee found to have violated this policy will be subject to disciplinary action, up to and including termination of employment. If a criminal offense is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

6.0 Definitions

- **Blogging:** Writing a blog. A blog (short for web log) is a personal online journal that is frequently updated and intended for general public consumption. This includes entries to social networking sites.
- **Spam:** Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History