




MONDI USER POLICY	
Policy Owner	Ed Montocchio
Effective Date	JUNE 2014
Policy no	PL14
Version	2

Table of Content

1.	Introduction.....	3
	a. Purpose	3
	b. Scope	3
2.	Policy.....	3
	a. General Use and Ownership	3
	b. Security and Proprietary Information	4
	c. Unacceptable Use	4
	d. System and Network Activities	4
	e. Information System Access Authority Form.....	5
3.	Policy Review	5
4.	Associated Documentation.....	5
5.	Functions Register	5
6.	Approved and Authorised Sign & Date.....	6

	MONDI USER POLICY	Policy Owner : Ed Montocchio
	IT SECURITY POLICY	Effective : 30 June 2014 Policy No : PL14.v2 Page 2 of 6

1. Introduction

a. Purpose

Mondi's intentions for publishing an Mondi User Policy are not to impose restrictions that are contrary to Mondi established culture of openness, trust and integrity. Mondi is committed to protecting Mondi's employees, partners and the company 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 Mondi. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Mondi employee and affiliate 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.

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


b. Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Mondi, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Mondi.

2. Policy

a. General Use and Ownership

- While Mondi'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 Mondi. Because of the need to protect Mondi's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Mondi.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. The Electronic Communications Policy provides guidelines concerning personal use of Email, Internet / Intranet / Extranet systems.
- For security and network maintenance purposes, authorized individuals within Mondi may monitor equipment, systems and network traffic at any time.

	MONDI USER POLICY	Policy Owner : Ed Montocchio
	IT SECURITY POLICY	Effective : 30 June 2014 Policy No : PL14.v2 Page 3 of 6

b. Security and Proprietary Information

- Keep passwords secure and do not share accounts. 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 10 minutes or less, or by logging-off (Ctrl-Alt-Delete) when the host will be unattended.
- Postings by employees from a Mondi email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Mondi, unless posting is in the course of business duties.
- 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.

c. 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 Mondi authorized to engage in any activity that is illegal under local, state or international law while utilizing Mondi-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.

d. 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 Mondi.
- 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 Mondi or the end user does not have an active license is strictly prohibited.
- 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.

	MONDI USER POLICY	Policy Owner : Ed Montocchio
	IT SECURITY POLICY	Effective : 30 June 2014 Policy No : PL14.v2 Page 4 of 6

- Using a Mondi 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 Mondi account.
- 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.
- Port scanning or security scanning is expressly prohibited unless prior notification to Mondi 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.
- 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, Mondi employees to parties outside Mondi.

e. Information System Access Authority Form

No access will be granted to any person unless an Information System Access Authority Form has been completed and authorized by the functional line manager. It is his / her responsibility to ensure that their staff is adequately trained to use the functions allocated.

3. Policy Review

IT Management has approved the Mondi User Policy; the policy will be reviewed annually.

4. Associated Documentation


PL3 Electronic Communication Policy

FRM1 Code of Conduct Confidentiality Form

FRM2 Information System Access Authority Form

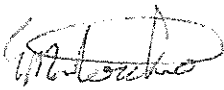
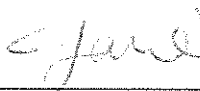

5. Functions Register


All IT Users

	MONDI USER POLICY	Policy Owner : Ed Montocchio
	IT SECURITY POLICY	Effective : 30 June 2014 Policy No : PL14.v2 Page 5 of 6

6. Approved and Authorised

Sign & Date

Policy Owner CIO		Ed Montocchio
CFO		Caroline Davie
CEO		Ron Traill

	MONDI USER POLICY	Policy Owner : Ed Montocchio
	IT SECURITY POLICY	Effective : 30 June 2014 Policy No : PL14.v2 Page 6 of 6