WELDO
Rebuilding Lives

Acceptable Use Policy

1 Overview

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

2 Purpose

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

3 Scope

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

4 Policy

4.1 General Use and Ownership

4.1.1 While WELDO'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 WELDO. Because of the need to protect WELDO's network, management cannot guarantee the confidentiality of information stored on any network device belonging to WELDO. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

4.1.2 WELDO recommends that any information that users consider sensitive or vulnerable be encrypted.

4.1.3 For security and network maintenance purposes, authorized individuals within WELDO may monitor equipment, systems and network traffic at any time.

4.1.4 WELDO reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 Before a user gains access to an WELDO computer, a general system use notice will be displayed that welcomes users and identifies it as a WELDO system, warns against unauthorized use of the computer, presents a privacy information banner as per GDPR, and indicates that your use of the system implies consent to all relevant WELDO policies.

4.2.2 Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System & User level passwords should be changed according to the "*Access Control Policy"*.

4.2.3 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 loggingoff (controlalt-delete for Windows users) when the host will be unattended.

4.2.4 Use encryption of information in compliance with WELDO's "*Encryption policy"*.

4.2.5 All hosts used by the employee that are connected to the WELDO Internet/Intranet/Extranet, whether owned by the employee or WELDO, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

4.2.6 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.

4.3 Unacceptable Use

4.3.1 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).

4.3.2 Under no circumstances is an employee of WELDO authorized to engage in any activity that is illegal under national or international law while utilizing WELDO-owned resources.

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

4.4 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

4.4.1 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 WELDO.

4.4.2 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 WELDO or the end user does not have an active license is strictly prohibited.

4.4.3 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4.4.4 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.

4.4.5 Using a WELDO 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.

4.4.6 Making fraudulent offers of products, items, or services originating from any WELDO account.

4.4.7 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

4.4.8 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.

4.4.9 Port scanning or security scanning is expressly prohibited unless prior notification to IT is made.

4.4.10 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.

4.4.11 Circumventing user authentication or security of any host, network or account.

4.4.12 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

4.4.13 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.

4.4.14 Providing information about, or lists of, WELDO employees to parties outside WELDO.

4.5 Email and Communications Activities

4.5.1 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).

4.5.2 Any form of harassment via email, telephone or SMS, whether through language, frequency, or size of messages.

4.5.3 Unauthorized use, or forging, of email header information.

4.5.4 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.

4.5.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4.5.6 Use of unsolicited email originating from within WELDO's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by WELDO or connected via WELDO's network.

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

4.6 Blogging

4.6.1 Blogging by employees, whether using WELDO’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 WELDO’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate WELDO’s policy, is not detrimental to WELDO’s best interests, and does not interfere with an employee's regular work duties. Blogging from WELDO’s systems is also subject to monitoring.

4.6.2 WELDO’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any WELDO confidential or proprietary information, trade secrets or any other material covered by WELDO’s Information Security policy when engaged in blogging.

4.6.3 Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of WELDO 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 WELDO.

4.6.4 Employees may also not attribute personal statements, opinions or beliefs to WELDO 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 WELDO. Employees assume any and all risk associated with blogging.

4.6.5 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, WELDO’s trademarks, logos and any other WELDO intellectual property may also not be used in connection with any blogging activity

5 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Definitions

Term:	Definition
Blogging:	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption. Blogging also includes writing or publishing on social media websites(like Facebook, Orkut etc.)
Spam:	Unauthorized and/or unsolicited electronic mass mailings.