Issuing Policy: Information Systems Department	Policy Originator: Erick Edstrom
Reviewed/Approved:	Reviewed/Approved:

Revision	Change Date	Originator	Description
Rev. 1	2014-06-10	Erick Edstrom	Initial

1.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and user accounts associated with Erica Lane Enterprises, Inc. information systems, including CheckPointHR, Erica Lane Enterprises, Inc. Timesheet, Email, Public website and the Employee Portal. These rules are in place to protect the employee and Erica Lane Enterprises, Inc. Inappropriate use of these systems may expose Erica Lane Enterprises, Inc. to risks including viruses, data integrity, system compromise and services, and possible legal actions.

2.0 Scope of Application

2.1 **Processes:** This policy applies to all information systems that is owned or leased by Erica Lane Enterprises, Inc. 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.

2.2 **Individuals/Organizations**: This policy applies to all employees, contractors, consultants, venders, and others accessing Erica Lane Enterprises, Inc. information systems, including all personnel affiliated with third parties.

2.3 **Exclusions:** None

3.0 References

3.1 **Corporate: Corporate Policy**

3.1.1 Password Policy
3.1.2 Email Policy
3.1.3 Software Installation Policy
3.1.4 Remote Access policy
3.1.5 Workstation Security Policy
3.1.6 Wireless Communication Device Policy

4.0 Definitions

4.1 **Blogging:** Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

4.2 **Spam:** Unauthorized and/or unsolicited electronic mass mailings.

4.3 **Denial-of-service attack:** Is an attempt to make a machine or network resource unavailable to its intended users.

5.0 Introduction

5.1 The intentions of this policy are not to impose restrictions that are contrary to Erica Lane Enterprises, Inc. established culture of openness, trust and integrity. We are committed to protecting Erica Lane Enterprises, Inc. employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. All company, personal and confidential employee data is protected information.

5.2 Effective security is a team effort involving the participation and support of every Erica Lane Enterprises, Inc. employee and affiliate who deals with information and/or information systems. It is the responsibility of every information systems user to know these guidelines, and to conduct their activities accordingly.

5.3 Unacceptable Use: Under no circumstances is an employee of Erica Lane Enterprises, Inc. authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Erica Lane Enterprises, Inc.-owned resources.

5.3.1 The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use. The following activities are strictly prohibited, with no exceptions:

5.3.1.1 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 Erica Lane Enterprises, Inc..

5.3.1.2 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 Erica Lane Enterprises, Inc. or the end user does not have a valid license is strictly prohibited.

5.3.1.3 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.

5.3.1.4 Introduction of malicious programs into any information system (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) is strictly prohibited.

5.3.1.5 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 performed remotely.

5.3.1.6 Using Erica Lane Enterprises, Inc. 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.

5.3.1.7 Making fraudulent offers of products, items, or services originating from any Erica Lane Enterprises, Inc. information system account.

5.3.1.8 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.

5.3.1.9 Port scanning or security scanning is expressly prohibited unless prior approval is received from the Information Systems Department.

5.3.1.10 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.

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

5.3.1.12 Interfering with or denying service to any user that utilizes information system resources (for example, denial-of-service attack).

5.3.1.13 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 remotely.

5.3.1.14 Providing any personal or confidential information about Erica Lane Enterprises, Inc. employees to parties outside of Erica Lane Enterprises, Inc. without consent from employee.

5.3.1.15 Using USB storage devices, CD ROM/DVD drives, and floppy drives unless prior approval is received from the Information Technology Department.

5.3.1.16 Sending or removing sensitive company or employee information from the premises of Erica Lane Enterprises, Inc., unless preapproved from an Erica Lane Enterprises, Inc. Executive.

5.3.1.17 Executing large downloads, streaming audio and video unless prior approval is received from the Information Systems Department.

5.3.1.18 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).

5.3.1.19 Any form of harassment via email, internet, telephone or texting, whether through language, frequency, or size of messages.

5.3.1.20 Sending company information to a personal email account is strictly prohibited, unless preapproved by an Erica Lane Enterprises, Inc. Executive.

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

5.3.1.22 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.

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

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

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

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

5.3.1.27 Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Erica Lane Enterprises, Inc. 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 Erica Lane Enterprises, Inc. Harassment policy.

5.3.1.28 Employees may also not attribute personal statements, opinions or beliefs to Erica Lane Enterprises, Inc. 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 Erica Lane Enterprises, Inc. Employees assume any and all risk associated with blogging.

5.3.1.29 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Erica Lane Enterprises, Inc. trademarks, logos and any other Erica Lane Enterprises, Inc. intellectual property may also not be used in connection with any blogging activity

6.0 Responsibilities

6.1 Managers and/or Supervisors will be responsible for monitoring employees to ensure compliance with this policy.

6.1.1 Management staff is expected to serve as role models for proper compliance with the provisions above and are encouraged to regularly remind employees of their responsibilities in this regard.

6.2 Information Systems Department is responsible for the review and updating of this policy as necessary.

6.2.1 While Erica Lane Enterprises, Inc. network administrations desire to provide a reasonable level of privacy, users should be aware that all data stored on Erica Lane Enterprises, Inc. information systems remains the property of Erica Lane Enterprises, Inc. Because of the need to protect Erica Lane Enterprises, Inc.'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to Erica Lane Enterprises, Inc.

6.2.2 For security and network maintenance purposes, authorized individuals within Erica Lane Enterprises, Inc. may monitor equipment, systems and network traffic at any time.

6.2.3 Erica Lane Enterprises, Inc. reserves the right to audit networks and systems on a periodic basis to ensure compliance with all Erica Lane Enterprises, Inc. policies.

6.2.4 Implementing physical and technical safeguards for all Erica Lane Enterprises, Inc. information systems to restrict access for unauthorized users.

6.3 Employees are responsible for:

6.3.1 Keeping your information systems usernames and passwords secure, authorized users are responsible for the security of their usernames and passwords.

6.3.1.1 Selecting a strong/complex password for each Erica Lane Enterprises, Inc. information system and must not be one that you use for a personal system or service logon.

6.3.1.2 Protecting all usernames and passwords, do not share Erica Lane Enterprises, Inc. usernames and passwords with anyone.

6.3.1.3 Not using the "Remember Password" feature on any application (e.g., Internet Explorer, Firefox, Safari, etc.).

6.3.1.4 If an account or password is suspected to have been compromised, report the incident to the Information Technology Department and change all passwords.

6.3.2 All devices must be secured with a password-protected screensaver/screen lock while unattended.

6.3.3 Because information contained on mobile devices is especially vulnerable, special care should be exercised.

6.3.3.1 Restricting physical access to only authorized personnel.

6.3.3.2 Physically secure device by using cable locks, locked drawers or cabinets.

6.3.4 Postings by employees from an Erica Lane Enterprises, Inc. email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Erica Lane Enterprises, Inc., unless posting is in the course of business duties.

6.3.5 All hosts used by the employee that are connected to the Erica Lane Enterprises, Inc. information systems, whether owned by the employee or Erica Lane Enterprises, Inc., shall be continually executing approved virus-scanning software with a current virus signature.

6.3.6 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.

6.3.7 Employees may not install software or hardware on any Erica Lane Enterprises, Inc. information systems.

6.3.8 In instances where the employee’s worksite has a more restrictive policy on information systems acceptable use in the workplace, the worksite’s policy should be used in addition to Erica Lane Enterprises, Inc. Corporate policy.

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