# PROFESSIONAL STANDARDS POLICY

**Title:** COMPUTER, EMAIL, INTERNET AND SOCIAL MEDIA USAGE

**Doc ID:** PS6005

**Revision:** 0.02

**Committee:** Professional Standards Committee

**Written by:** J. Brown, R. Anderson

**Notes:** Guidelines for Computer, Email, Internet, and Social Media for ECI Staff

**Date Established:**     March 2015

**Date Last Revised:**     October 2022

**Next Revision Review:** October 2027

**Approved by:**     Board of Directors

## Table of Contents

## Policy Statement

Use of the Internet by employees, volunteers, committee members, and Board of Directors of EnviroCert International, Inc. (ECI or EnviroCert) is permitted and encouraged where such use supports the goals and objectives of the organization. However, all employees must adhere to the requirements specified in this policy concerning computer, email and Internet usage. Violation of these policies could result in disciplinary and/or legal action leading up to and including termination of employment. Employees may also be held personally liable for damages caused by any violations of this policy. All employees are required to acknowledge receipt and confirm that they have understood and agree to abide by the rules hereunder.

## BACKGROUND

This policy provides employees, volunteers, committee members, and Board of Directors with rules and guidelines about the appropriate use of computing equipment, data networks and Internet access. This policy helps to protect both ECI and its employees from issues arising from unauthorized use of corporate computing and networking resources.

## PURPOSE

ECI provides access to the vast information resources of the Internet to help you do your job and be well-informed. The facilities and equipment that provide access represent a considerable commitment of resources for telecommunications, networking, software, storage, etc. This policy is designed to help you understand the expectations for the use of those resources and to help you use those resources wisely.

## APPLICABILITY

This Computer, Email and Internet Usage Policy applies to all EnviroCert employees, volunteers, and Board of Directors who have access to computers and the Internet in the course of performing their work assignments.

## DEFINITIONS

Computer: An electronic device for storing and processing data according to programmed instructions. In the context of this policy, the term computer includes tablet computers, smartphones, and similar devices capable of accessing corporate Internet resources.

Email: Messages distributed by electronic means from one computer to one or more recipients via a network.

Instant message: Messages sent via the Internet that appear on the recipient's computer as

soon as it is transmitted.

Internet:  A global electronic communications network that connects computer networks and organizational computer facilities around the world.

Social Media:  Websites and applications that enable users to create and share content or to participate in social networking

Text Message:  A short message sent electronically especially from one mobile phone to another.

## RESPONSIBILITY

### Executive Director

The EnviroCert Executive Director is responsible for the following items:
- Reviewing this policy with each employee annually
- Investigating and resolving violations of this policy
- Providing a summary report to the Board of Directors on compliance issues

### Administrative Manager

The Administrative Manager is responsible for the following items:
- Storing the signed agreements in each employee's human resources file
- Assisting the Executive Director with investigations (as requested)

### Employees

Each EnviroCert employee is responsible for the following items:
- Understanding and complying with the requirements of this policy
- Signing the agreement contained in Appendix A of this policy

## HISTORY AND UPDATE

This document represents the first version of the Policy and Procedure.

## Procedures

### A.  Computer, Email and Internet Usage

- Company employees, volunteers, committee members, and Board of Directors are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities.

- Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role.

- All Internet data that is composed, transmitted, and/or received by ECI's computer systems is considered to belong to EnviroCert and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

- The equipment, services, and technology used to access the Internet are the property of ECI and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent, or received through its online connections.

- Emails and other forms of electronic communication (such as text messages, instant messages, and social media) sent via the company EnviroCert-provided equipment should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images

- All sites and downloads may be monitored and/or blocked by ECI if they are deemed to be harmful and/or not productive to organization

- The installation of software by employees is prohibited with the exception of routine updates to EnviroCert-provided software.


B. **Unacceptable Use of the Internet or Social Media by Employees Includes, But Is Not Limited To:**

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via ECI's email service

- Sending, posting, or storing pornographic or sexually explicit messages or images on the Internet, local computer, server, or via EnviroCert's email service

- The storage of personal files or use for activities not related to ECI related events and organization is not permitted.

- Using computers to perpetrate any form of fraud, and/or software, film or music piracy

- Stealing, using, or disclosing someone else's password without authorization

- Downloading, copying, or pirating software and electronic files that are copyrighted or without authorization

- Sharing confidential material, trade secrets, or proprietary information outside of the organization

- Hacking into unauthorized websites

- Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers

- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems

- Sending or posting chain letters, solicitations, or advertisements not related to organization purposes or activities

- Passing off personal views as representing those of the organization

- Using reproduction, printers, supplies, other resources for personal use not approved by ECI.

If an employee is unsure about what constitutes acceptable usage under this policy, then he/she should ask his/her supervisor for further guidance and clarification.


## C. Social Media Policy

- Social media includes any form of electronic communication including, without limitation, posting, or communicating on the Internet to an employee's or someone other than an employee's blog, discussion forums, social networks, and web sites.

- An employee should adhere to the same principles that are found in Company's employment policies when participating in social media.  In particular, an employee should adhere to the guidelines in the Violence and Harassment Policies when posting online.  Postings by an employee such as statements that discriminate based on characteristics protected by law, visuals or comments that are sexually harassing and threats that are violent in nature or any other conduct that is improper or illegal may subject the employee to disciplinary action, up to and including termination.

- When posting online, an employee should:

  o Be respectful and considerate of Company's employees, customers, and suppliers.

  o Refrain from using social media that could be viewed as harassing, malicious, lewd, threatening, or that denigrates other employees, customers or suppliers when posting complaints or criticism.  Examples of such behavior includes bullying using racial slurs or taunts or other comments based on a status protected by law such as

religion, sex, or disability or posting derogatory remarks that have the intent to damage a person's reputation.

o   Preserve the confidentiality of Company's confidential or proprietary information such as internal business reports and financial information and Company's trade secrets.  Trade secrets may include information related to bidding, marketing plans, internal processes, and system designs.

o   State only the employee's personal opinions and refrain from representing that the employee is communicating on behalf of the Company.  To make clear that the employee is not posting on the Company's behalf, the employee should consider the use of a disclaimer such as, "The views expressed on this [website] [blog] are mine alone and may not reflect the views of EnviroCert International, Inc."

o   Refrain from the use of social media during work time or on equipment provided by the Company unless otherwise authorized by the employee's supervisor.

## Related Documents

**ECI Documents:**
  Employee Manual
  Administrative Handbook

**Other Documents:**
  N/A

**Related Links:**
  N/A

## Appendix A

Your signature below indicates that you thoroughly understand and accept these policies as a material condition of your employment and that any violation of any of these provisions may result in disciplinary action that may include immediate termination.

EnviroCert International, Inc.

Name (please print):        Robert W. Anderson

Title:                      Executive Director

Date:

Signature:

Employee

Name (please print):

Date:

Signature: