Acceptable Use Policy

Author: ECWI Security Team

Date: 7th August 2014

Review History				
Name	**Department**	**Role/Position**	**Date approved**	**Signature**

Approval History				
Name	**Department**	**Role/Position**	**Date approved**	**Signature**

1 Overview

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at ECWI in conjunction with its established culture of ethical and lawful behaviour, openness, trust, and integrity.

ECWI provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

2 Scope

All employees, contractors, consultants, temporary and other workers at ECWI, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by ECWI, or to devices that connect to a ECWI network or reside at a ECWI site.

Information Security must approve exceptions to this policy in advance.

3 Policy Statement

3.1 General Requirements

3.1.1 You are responsible for exercising good judgment regarding appropriate use of ECWI resources in accordance with ECWI policies, standards, and guidelines. ECWI resources may not be used for any unlawful or prohibited purpose.

3.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic per the Audit Policy. Devices that interfere with other devices or users on the ECWI network may be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

3.2 System Accounts

3.2.1 You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

3.2.2 You must maintain system-level and user-level passwords in accordance with the Password Policy.

3.2.3 You must ensure through legal or technical means that proprietary information remains within the control of ECWI at all times. Conducting ECWI business that results in the storage of proprietary information on personal or non-ECWI controlled environments, including devices maintained by a third party with whom ECWI does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by ECWI, or its customer and partners, for company business.

3.3 Computing Assets

3.3.1 You are responsible for ensuring the protection of assigned ECWI assets that includes the use of computer cable locks and other security devices. Laptops left at ECWI overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of ECWI assets to the ECWI Security Team.

3.3.2 All PCs, PDAs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

3.3.3 Devices that connect to the ECWI network must comply with the Minimum Access Policy.

3.3.4 Do not interfere with corporate device management or security system software, including, but not limited to antivirus.

3.4 Network Use

You are responsible for the security and appropriate use of ECWI network resources under your control. Using ECWI resources for the following is strictly prohibited:

3.4.1 Causing a security breach to either ECWI or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.

3.4.2 Causing a disruption of service to either ECWI or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

3.4.3 Introducing honeypots, honeynets, or similar technology on the ECWI network.

3.4.4 Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.

3.4.5 Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.

3.4.6 Use of the Internet or ECWI network that violates ECWI policies, or local laws.

3.4.7 Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.

3.4.8 Port scanning or security scanning on a production network unless authorized in advance by Information Security.

3.5 Electronic Communications

The following are strictly prohibited:

3.5.1 Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates ECWI policies against harassment or the safeguarding of confidential or proprietary information.

3.5.2 Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

3.5.3 Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

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

3.5.5 Use of a ECWI e-mail or IP address to engage in conduct that violates ECWI policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a ECWI e-mail or IP address represents ECWI to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

4 References

- FIRST.ORG
  `https://www.first.org/_assets/resources/guides/aup_generic.doc`

5 Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with ECWI.

6 Definitions

Term	Definition
honeypot, honeynet	Network decoys that serve to distract attackers from valuable machines on a network. The decoys provide an early warning for intrusion detection and detailed information on vulnerabilities.
Spam	Electronic junk mail or junk newsgroup postings. Messages that are unsolicited, unwanted, and irrelevant.

7 Revision History

Date of Change	Responsible	Summary of Change