

# Acceptable Use Policy

## 1. Overview

Ocwen's intentions for publishing the *Acceptable Use Policy* are not to impose restrictions that are contrary to Ocwen's established culture of openness, trust, and integrity. Ocwen is committed to protecting employees and partners 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 Ocwen. 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. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Ocwen 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.

## 2. Purpose

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

## 3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Ocwen business or interact with internal networks and business systems, whether owned or leased by Ocwen, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Ocwen and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Ocwen's *Acceptable Use Policy*.

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

## 4. Policy

### 4.1 General Use and Ownership

- 4.1.1 Ocwen's proprietary information stored on electronic and computing devices, whether owned or leased by Ocwen, the employee, or a third party, remains the sole property of Ocwen. You must ensure through legal or technical means that proprietary information is protected in accordance with Ocwen's *Data Protection Standard*.
- 4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Ocwen proprietary information.
- 4.1.3 You may access, use, or share Ocwen proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- 4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- 4.1.5 For security and network maintenance purposes, authorized individuals within Ocwen may monitor equipment, systems, and network traffic at any time.
- 4.1.6 Ocwen 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 All mobile and computing devices that connect to the internal network must comply with Ocwen's *Minimum Access Policy*.
- 4.2.2 System-level and user-level passwords must comply with Ocwen's Password Policy. Providing access to another individual, either deliberately or through failure to secure the device's access, is prohibited.
- 4.2.3 All computing devices 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.
- 4.2.4 Postings by employees from an Ocwen-owned/leased computing device to personal social media accounts is strictly prohibited.
- 4.2.5 Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware.

### 4.3 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 Ocwen authorized to engage in any activity that is illegal under local, state, federal, or international law while using Ocwen-owned resources.

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

#### 4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

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 Ocwen.
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 Ocwen or the end user does not have an active license, is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting Ocwen business, even if you have authorized access, is prohibited.
4. 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. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
6. 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.

7. Using an Ocwen 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.
8. Making fraudulent offers of products, items, or services originating from any Ocwen account.
9. 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.
10. Port scanning or security scanning is expressly prohibited unless prior notification to the Ocwen IT Security department is made.
11. Executing any form of network monitoring that will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network, or account.
13. Introducing honeypots, honeynets, or similar technology on the Ocwen network.
14. Interfering with or denying service to any user other than the employee's host (for example, denial-of-service attack).
15. 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.
16. Providing information about, or lists of, Ocwen employees to parties outside Ocwen.

#### 4.3.2 Email and Communication Activities

When using company resources to access and use the internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that “the opinions expressed are my own and not necessarily those of the company.” Questions may be addressed to the IT Department.

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).
2. Any form of harassment via email and telephone, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
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.
5. Creating or forwarding “chain letters,” “Ponzi,” or other “pyramid” schemes of any type.
6. Use of unsolicited email originating from within Ocwen’s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Ocwen or connected via Ocwen’s network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

#### 4.3.3 Blogging and Social Media

1. Blogging by employees, whether using Ocwen’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 Ocwen’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Ocwen’s policy, is not detrimental to Ocwen’s best interests, and does not interfere with an employee’s regular work duties. Blogging from Ocwen’s systems is also subject to monitoring.
2. Ocwen’s *Confidential Information Policy* also applies to blogging. As such, employees are prohibited from revealing any Ocwen confidential or proprietary information, trade secrets, or any other material covered by Ocwen’s *Confidential Information Policy* when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation, and/or goodwill of Ocwen 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 Ocwen's *Non-Discrimination and Anti-Harassment Policy*.
4. Employees may also not attribute personal statements, opinions, or beliefs to Ocwen 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 Ocwen. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Ocwen's trademarks, logos, and any other Ocwen intellectual property may also not be used in connection with any blogging activity.

## 5. Policy Compliance

### 5.1 Compliance Measurement

The IT Security team will verify compliance to this policy through various methods, including, but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

### 5.2 Exceptions

Any exception to the policy must be approved by the IT Security team in advance.

### 5.3 Non-Compliance

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

## 6. Related Standards, Policies, and Processes

- Confidential Information Policy
- Data Classification Policy
- Data Protection Standard
- Minimum Access Policy
- Non-Discrimination and Anti-Harassment Policy
- Password Policy
- Social Media Policy