Important Note to User: This is a sample agreement is not a "one-size-fits-all" and should not be used by any organization without review and modification to fit the needs of such organization. Organizations should cross-reference with relevant existing policies where appropriate, comparing against relevant policies (e.g. mobile device and acceptable use policies), ensuring terms are defined consistently across policies. Additional changes to this agreement may be necessary to account for varying individual organizational security needs and user privacy expectations. In addition, while efforts have been made to ensure that the terms of this policy comply with employee rights under the National Labor Relations Act, this is a contentious and ever changing area of the law, and therefore total compliance cannot be guaranteed. **Delete this note before publishing.**

Sample Organization Acceptable Use Policy

Establishment date, effective date, and revision procedure

This policy was established and approved by [Organization Name] on mm,dd,yyyy. The [Organization Name] Information Security department shall review this policy at least once a year, and at any additional time when there are changes that may affect corporate management with respect to Information Security. In the event that amendment or repeal of this policy becomes necessary as a result of such review, the [Organization Name] Information Security department shall prepare a draft and apply for authorization, and with prior confirmation of the Executive(s) in charge of the area(s) that will be affected by amendment or repeal, the [Organization Name] CISO/Security Director will authorize the amendment or repeal.

Table of revision history

Version	Date	Details of change	Issued by	Approved by

© 2016 ePlace Solutions, Inc.

Overview

Effective information security requires the support and participation of all employees and affiliates of [Organization Name] who deal with company information and/or information systems. All computer users within the company are responsible for reading and following the guidelines set forth below. Pease review your Employee Handbook for further details.

Purpose

This policy describes the acceptable use of [Organization Name]'s computer equipment. By complying with the directives set forth below, employees help to protect [Organization Name] from risk of malware attacks, compromise of network systems and services, and legal liability.

Scope

This policy applies to employees, contractors, consultants, volunteers, temporary and other workers at [Organization Name], and all personnel affiliated with company subsidiaries or third parties. This policy applies to all equipment that is owned or leased by, or otherwise in the custody or control of, [Organization Name].

This policy applies to the use of all information, electronic and computing devices, and network resources used by [Organization Name] to conduct business or interact with internal networks and business systems, whether owned or leased by, or otherwise in the custody or control of, [Organization Name], the employee, a company subsidiary, or a third party.

Policy

All employees, contractors, consultants, volunteers, temporary and other workers at [Organization Name], and all personnel at company subsidiaries and third-parties are responsible for exercising good judgment regarding appropriate and reasonable use of information, electronic devices, and network resources in a manner that complies with [Organization Name]'s policies and procedures, and local laws and regulations.

General Use and Ownership

1. [Organization Name]'s proprietary information created and/or stored on electronic and computing devices whether owned or leased by, or otherwise in the custody or control of, [Organization Name], the employee, or a third party, remains the sole property of [Organization Name].

2. Employees have a responsibility to promptly report the theft, loss or unauthorized disclosure of [Organization Name] trade secrets, or proprietary or confidential information such as information relating to product development, organizational security measures, and business, financial, or marketing strategies.

3. Employees may access, use or share [Organization Name]'s trade secrets and proprietary information such as customer lists and contact information, development of systems, processes, products, know-how, technology and internal reports and procedures, only to the extent it is authorized and necessary to fulfill their assigned job duties or in limited circumstances where such access, use, or disclosure is protected under the National Labor Relations Act and is compliant with applicable laws.

© 2016 ePlace Solutions, Inc.

4. All employees are responsible for exercising good judgment regarding the reasonableness of their personal use. Individual departments are responsible for creating their own guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such guidelines, employees should consult their supervisor or manager.

5. All information considered sensitive or vulnerable must be encrypted. Such information includes but is not limited to employee personal information, customer lists and contact information, and [Organization Name] trade secrets and proprietary or confidential information.

6. In order to maintain the security and integrity of company systems and networks, authorized individuals within [Organization Name] may monitor electronic and computing equipment, systems, and network traffic at any time.

7. [Organization Name] reserves the right to audit all electronic and computing equipment, networks, and systems on a periodic basis to ensure compliance with this policy.

8. Employees and users of [Organization Name] equipment are expected to take charge of their own training by attending in-house classes provided by the IT department, and reviewing and becoming familiar with software documentation.

Security and Proprietary Information

1. Mobile and computing devices that connect to the internal network will be limited to the minimum access necessary to conduct business in order to protect [Organization Name]'s sensitive, proprietary, or confidential information from potential compromise. However, nothing in this paragraph shall be construed to interfere with or restrict employee rights under the National Labor Relations Act.

2. All system level and user level passwords must comply with the security requirements of the *Access Control Policy*. Employees are prohibited from providing any other individual access to company networks and systems, either intentionally or through failure to take reasonable steps to secure their access.

3. All computing devices must be secured with a password-protected screensaver that activates automatically after 10 minutes or less. Employees must manually lock the screen or log off when leaving their computing device unattended.

4. Employees must use extreme caution and comply with the safeguards in [Organization Name]'s *Email Policy* when opening e-mail attachments received from unknown senders, which may contain malware.

5. Employees must safeguard all [Organization Name] equipment assigned to their exclusive or shared use, and all [Organization Name] equipment within their work area.

6. Employees traveling with [Organization Name] laptop computers must always carry them in carry-on baggage and not in checked baggage.

© 2016 ePlace Solutions, Inc.

Unacceptable Use

The following activities are prohibited. Employees may be exempted from certain restrictions where required to engage in legitimate job responsibilities (e.g., systems administration staff may need to engage in specified restricted activity in order to test company security vulnerabilities or to disable the network access of a host if that host is disrupting production services). Employees may also be exempted from specific restrictions in limited circumstances where activities are protected by the National Labor Relations Act.

Employees are prohibited from engaging in any activity that is illegal under local, state, federal or international law while utilizing [Organization Name]-owned resources.

The lists below are not exhaustive, but attempt to provide guidance on what activities fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited:

1. Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property laws and regulations, including, but not limited to, installing or distributing "pirated" or other software products for which the [Organization Name] lacks an appropriate license.

2. Unauthorized and unlawful reproduction of materials protected by copyright including activities such as digitization and distribution of photographs from magazines, books, online databases, or other similar copyrighted sources, copyrighted music, and the installation of any copyright protected software for which [Organization Name] or other end user lacks a valid license.

3. Accessing data, a server or an account for any purpose other than conducting [Organization Name] business or for limited activities protected by the National Labor Relations Act, such as union organizing or other protected concerted activities.

4. Exporting technical information, software, or encryption software or technology, in a manner prohibited by international or regional export control laws. Employees should consult management prior to exporting any material that is in question.

5. Introducing malicious programs into company networks or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, suspicious packers, etc.).

6. Disclosing account passwords to others or allowing others to access and use your account in any manner. This includes access or use by family and other household members when working from home.

7. Using a [Organization Name] computing device to procure or transmit material that is in violation of the organization’s anti-discrimination and harassment policies and state and federal laws.

8. Using any [Organization Name] account to make fraudulent offers of products, goods, or services.

© 2016 ePlace Solutions, Inc.

9. Making statements about warranty, expressly or implied, of any product, good, or service unless such statements are part of legitimate job duties.

10. Effecting security breaches or disruptions of network communication or services. 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 such activities are within the scope of regular business duties or otherwise permitted by law. For purposes of this section, "disruption" includes, but is not limited to, bulk email or spam, denial of service, packet spoofing, network sniffing, pinged floods, and forged routing information for malicious purposes.

11. Using any form of network monitoring that intercepts data not intended for the employee's host, unless this activity is a part of legitimate job duties.

12. Bypassing user authentication and/or security of any host electronic or computer device, network, or account owned by [Organization Name].

13. Disabling anti-virus software on workstations or devices.

14. Interfering with or denying service to another user's host (for example, denial of service attack).

15. Sending any messages such as programs, scripts, or commands with the intent to cause interference of, or disable, a user's terminal session, by any means, whether locally or via the Internet/Intranet/Extranet.

16. Disclosing information about, or lists of [Organization Name]'s employees to customers, competitors, or other similar parties outside of [Organization Name].

17. Hacking systems and databases or acting to disrupt systems or cause unnecessary network congestion or application delays.

18. Using remote control or remote access software on any internal or external host personal computers or systems not specifically set up by the IT staff.

19. Using [Organization Name] equipment for personal profit, political fundraising, gambling activity, non-business-related instant messaging or chat room discussions, or downloading or displaying of offensive material, unless such fundraising or messaging activity is for the limited purpose of exercising employee rights under the National Labor Relations Act, such as union organizing or other protected concerted activity.

20. Browsing pornographic, offensive, or otherwise undesired and questionable sites on the internet which may result in introduction of malicious programs into the company's network or server.

Email and Communication Activities

Employees are perceived to represent the company when they use company resources to access the Internet. To avoid confusion, during online communications unrelated to legitimate work responsibilities, whenever employees state an affiliation to the company, they are encouraged to clearly indicate the following: "I do not represent the company in any manner. Any opinions

© 2016 ePlace Solutions, Inc.

expressed on this matter are my own and not necessarily those of the company". However, such disclosure is not required for limited communications protected by the National Labor Relations Act. Questions concerning such disclosures should be addressed to the IT or HR Departments.

The following email activities are strictly prohibited:

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), except in limited circumstances where such communication is protected by the National Labor Relations Act, such as union organizing or other protected concerted activity.

2. Any form of unlawful harassment via email, telephone or paging, whether perceived as harassment through language, frequency, or size of messages.

3. Unauthorized use, misappropriation, or forging of information in email headers.

4. Solicitation of emails for another email address, other than that of the poster's account, with the intent to unlawfully harass or collect replies.

5. Creating or forwarding harassing and unwanted "chain letters", "Ponzi", or other "pyramid" schemes of any type regardless of content, sources, or destinations. Nothing in this paragraph will be construed to limit employees from engaging in legitimate protected concerted activity under the National Labor Relations Act.

6. Posting [Organization Name] proprietary or confidential information such as product development, organizational security measures, and business, financial or marketing strategies to external newsgroups, bulletin boards, or other public forums without authority.

7. Any use of unsolicited emails obtained from within [Organization Name]'s networks that were sent by other Internet/Intranet/Extranet service providers on behalf of, or to advertise, services hosted by [Organization Name] or connected via [Organization Name]'s network.

8. Posting non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam) or other similar abusive tactics.

Blogging and Social Media

1. Blogging by employees, whether using [Organization Name]’s property and systems or personal computer systems, when used to carry out job responsibilities, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of [Organization Name]’s systems to engage in blogging related to legitimate job-related responsibilities is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate [Organization Name]’s policy, is not detrimental to [Organization Name]’s best interests or image, and does not interfere with an employee's regular work duties. However, nothing in this paragraph shall be construed to limit employees’ rights to discuss the terms and conditions of their employment or to engage in other legitimate protected concerted activities under the National Labor Relations Act. Employees should also note that blogging from [Organization Name]’s systems is subject to monitoring.

2. Employees shall not engage in any blogging whether during the course of business duties or after working hours that unlawfully defames or maligns the image, reputation and/or goodwill of [Organization Name] and/or any of its employees. Employees are also prohibited from making

© 2016 ePlace Solutions, Inc.

any discriminatory, disparaging, defamatory, harassing, or otherwise unlawful comments when blogging, or otherwise engaging in any conduct prohibited by [Organization Name]'s *Anti-Discrimination and Harassment* policy.

3. Employees may not hold themselves out as representatives of the company or attribute personal statements, opinions or beliefs to [Organization Name] when engaged in blogging or posting to newsgroups, or other social media. If an employee expresses his or her beliefs and/or opinions in blogs or social media posts, the employee is encouraged to disclose the following: "I do not represent the company in any manner. Any opinions expressed on this matter are my own and not necessarily those of the company". However, where engaging in limited activity protected by the National Labor Relations Act, such as discussing terms and conditions of employment, employees need not provide such disclosure. Employees who engage in blogging outside the scope of their job duties assume any and all associated risk.

4. [Organization Name]'s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any [Organization Name] confidential or proprietary information or trade secrets such as product development, organizational security measures, and business, financial or marketing strategies, or any other material designated as confidential when engaged in blogging.

5. In addition to following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, [Organization Name]'s trademarks, logos and any other [Organization Name] intellectual property may also not be used in connection with any blogging activity except in limited circumstances where such use is protected by the National Labor Relations Act. In all circumstances, employees must comply with all applicable copyright, trademark, and other similar intellectual property laws.

Policy Compliance

Compliance Measurement

Compliance with this policy will be verified by [Organization Name] through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the [Policy Owner].

Exceptions

Any exception to the policy must be approved by the [Policy Owner] in advance.

Non-Compliance

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

© 2016 ePlace Solutions, Inc.