Zuora Acceptable Use Policy

Version 2.2 - Last Updated 03 August 2021

Confidentiality

This Acceptable Use Policy is intended solely for use by internal Zuora personnel, contractors, and temporary workers, and Zuora business partners. Zuora's current and prospective customers that have completed a non-disclosure agreement with Zuora may review this document.

This Acceptable Use Policy is Zuora's confidential and proprietary information. Unauthorized use, reproduction, or distribution of this document, in whole or in part, is strictly prohibited.

Zuora reserves the right, at its sole discretion, to change, modify, add or remove portions of this Acceptable Use Policy at any time.

Table of Contents

1. POLICY

Zuora is committed to protecting customers, staff, and partners from illegal or damaging actions by individuals, either knowingly or unknowingly. This Acceptable Use Policy ("**Policy**" or "**AUP**") is intended to protect Zuora's culture of openness, trust and integrity while also ensuring effective security over its systems and protecting Zuora's and its customers' information. This is a team effort that requires the participation and support of every ZEO.

It is the responsibility of every User to know these guidelines, and to use Computing Systems accordingly.

We are looking for all ZEOs to do their part to protect Zuora's Computing Systems.

2. PURPOSE

The purpose of this Policy is to outline the acceptable use of Computing Systems at Zuora and when applicable, the monitoring Zuora related communications by ZEOs. This Policy is in place to ensure all Users use the Computer Systems in an effective, safe, efficient, ethical and lawful manner. Inappropriate use of the Computing Systems may expose Zuora to risk from network compromises to theft of Zuora's (or our Customers') information, data, and work product.

3. SCOPE AND AUDIENCE

3.1 Scope

As a part of its operations, Zuora uses numerous technologies, systems, third party tools, along with other information assets and processes ("**Computing Systems**") such as:

- Zuora issued mobile devices, such as laptops, smartphones and tablets ("**Mobile Device**");
- Zuora provided access to:
  - wireless networks
  - intranet systems
  - third party platforms, programs, tools or SaaS products ("**Third Party Tools**")
- Remote access/VPN to any Computing System
- Internet access and use within a Zuora location or using a Mobile Device

- Removable media containing Zuora information, whether or not such media was provided by Zuora
- Computing facilities
- Office key cards
- Office printers/fax machines
- Office telephone systems
- Electronic communication systems, and computing facilities
- Any information, data, or messages created, received, sent or stored in any Computing System
  - Communications among Users along or with Zuora customers, prospects, and contacts using any Computing System
  - Voicemail and e-mail, along with related hardware and software
  - Correspondence created or sent using a Computing System
  - Tools to schedule, conduct and/or record meetings and telephone conversations

The Computing Systems as a whole, along with any information, data, assets and messages created, received, sent or stored within any individual Computing System, are Zuora's property.

3.2 Audience

All Zuora employees, contractors, consultants, agents and affiliates ("**ZEOs**" or "**Users**") must adhere to this Acceptable Use Policy.

4. ROLES AND RESPONSIBILITIES

- Security Team is responsible for developing, reviewing, and overseeing this Policy.
- Managers, in cooperation with the Security Team, are responsible for training Users on this Policy and documenting compliance issues.
- Information Technology Team is responsible for overseeing Computing System integrity; along with monitoring, and reporting Users actions relating to Computing Systems and facilities.
- Human Resources Team is responsible for conducting global coordination and is the custodian of relevant forms.
- Senior Executive Management is responsible for conducting reviews of this Policy and its enforcement.
- All Users are required to understand, acknowledge, and adhere to the terms of this Policy.

5. POLICY DIRECTIVES

5.1 Acknowledgement Form

Upon joining Zuora and upon a periodic basis thereafter, Users will receive a copy of this Policy along with a form acknowledging that the User has read the Policy and will adhere to its terms and conditions. Zuora may update this Policy from time to time. Users are required to review and agree to adhere to the Policy at least annually. A copy of this Policy will be accessible on Zuora's intranet.

5.2. Maintaining System Integrity

As applicable, Computing Systems shall be configured by the Information Technology (IT) Department according to Zuora's standard processes and requirements. Users shall not make changes to any platform or platform standard, modify the hardware configuration, or operating system unless authorized by the IT Department. Users may be responsible for damages resulting from unauthorized changes to any Computing System they caused. As applicable, the following tools will be installed on each User's Computing System:

- Screensaver requiring a password entry after 15 minutes of inactivity.
- Anti-virus, Anti-spam software.
- JAMF or other device profile monitoring utilities.
- Personal firewall software.
- Encryption software when applicable to the user job function.

Users shall use these tools as appropriate for their position and immediately report any faulty or non-existent instances of these tools to the Security Team and/or IT Department.

Users are responsible for protecting the Computing Systems and complying with this AUP. Users are responsible for notifying the Security (security@zuora.com/ #zsecurity) and or the IT (zeus@zuora.com/ #it) teams as appropriate in cases of computer anomalies and incidents.

Users are also responsible for complying with the Zuora Information Security Policy, Password Policy, and any other accompanying policies as designated by the Security Team which can be accessed from Zuora's intranet page. Users shall exercise reasonable care to protect the Computing Systems. Users may not use passwords for Computing Systems across different platforms regardless if the respective password is meant for internal or external use or otherwise used for

professional or personal purposes. For example, a User's passwords for Okta, work Gmail, and personal Gmail should never be the same.

5.3. Monitoring

All Users are monitored by Zuora whenever they are using the Computing Systems. All Users' communications and actions may be recorded, tracked, or similarly processed by Zuora without providing additional notice. For example, Zuora may

- Review and store data relating to use of Computing Systems by an individual User;
- Monitor websites that a User visits, e-mails exchanged on a Zuora-provided e-mail account or a personal e-mail account accessed from a Mobile Device or Computing System;
- Track and locate Users' Computing Systems, including, but not limited to, in the event a Computer System has been either lost or stolen; and
- Review Users' instant messenger sessions and, if applicable to a User's position at Zuora, record the User's telephone conversations.

5.4. Unacceptable Use

5.4.1. General Requirements

- Users are responsible for exercising good judgment regarding appropriate use of Computing Systems in accordance with Zuora's policies, procedures, and guidelines. Computing Systems may not be used for an unlawful, prohibited or personal purpose.

- Users are prohibited from providing information about ZEO employees or Zuora customers (including, but not limited to lists containing names of ZEOs), to parties outside of Zuora, except with prior authorization from the Human Resources Department or Legal Team.

5.4.2. System Accounts and Access

- Users shall not share their individual Computing System account information, passwords, security tokens (i.e., Google authenticator), or similar information or devices used for individual User identification and authorization purposes.
- Users shall not store (or take offsite) any Zuora customer data. For more information, please review Information Security Policy.

- Users shall not send Zuora customer data, personally identifiable information (PII), protected health information (PHI), personal data, personal information, or Primary Account Number (PAN) information using end-user messaging technologies, such as e-mail, instant messaging, or chat.
- Users should not attempt to access any Computing System for which they have not been authorized.

5.4.3. Software

- Users shall not run or install any program or software without approval of the Security Team. This includes, but is not limited to, any malicious programs such as computer viruses, Trojan horses, worms, and malware.
- Users shall not use Peer-2-Peer file-sharing software unless authorized by the Security Team. This includes any software that may violate copyright laws (such as, Kazaa, BitTorrent, Limewire).
- Users shall not duplicate any copyrighted software, except as permitted by the Security Team (in consultation with the Legal Team).
- Users shall not use any Computing System to create, host, or transmit material which infringes copyright, trademark, patent, trade secret, or other proprietary rights of another.
- Users shall not download, install, run or operate any program, software, or utility on a Computing System unless authorized by the Security Team.
- A User may not attempt to reveal weaknesses in the security of any Computing System unless required based on Zuora role responsibilities.
- Users may only use authorized software or applications for transmitting, processing, or storing of Zuora information assets and customer data.

5.4.4. Network Use

- A User shall not use packet sniffing, packet flooding, spoofing, network scanning, denial of service and forging routing information for malicious purposes unless required to Zuora role responsibilities.
- Users should not connect unauthorized equipment or networks to any Computing System or facilities. The Security Team must pre-authorize any equipment that a User seeks to connect to any Computing System, including the Zuora network. (Exceptions to this are standard computer peripheral devices for personal use that do not capture, store, and or process Zuora Data such as keyboards, computer mouse, external displays, printers.)
- Users should not interfere with the normal operation of Computing Systems, including individual computers, terminals, peripherals, or networks.
- Users should not attempt to monitor or tamper with another User's Computing Systems. This includes reading, copying, changing or deleting another User's communications, files or software unless explicitly authorized by Zuora.

5.4.5. Electronic Communications and Publicity

- Users should not use a Zuora-provided e-mail address for any purpose other than for business or professional purposes. All Users are accountable for their actions using a Computing System.
- Users should not forge, misrepresent, obscure, or replace their User-information on any electronic communication for any reason, including to mislead the recipient.
- Users should not directly communicate with the press concerning Zuora or discuss Zuora information in public forums or using social media. All external inquiries regarding Zuora's business should be routed to press@zuora.com.

5.4.6. Computing Systems

- Users should not use Computing Systems for activity outside of legitimate Zuora business.
- Users should not send or store fraudulent, harassing, defamatory, offensive, indecent or obscene messages from or on any Computing System.
- Users are prohibited from sending Spam or other unsolicited e-mail, chain letter, or other form of mass mailing from Computing Systems.
- Users are prohibited from using any Computing System to solicit support for religious or political causes or for personal financial gain.

5.4.7. Computing System , Zuora Assets, and "Clean Desk" Policy

- Users should not modify the hostname of their Mobile Devices.
- Users must securely store assigned Mobile Devices , including when leaving Mobile Devices overnight in a Zuora facility. Users should always place Mobile Devices in a locked drawer or cabinet.
- Users should not leave confidential information on printers, photocopiers, or otherwise unprotected within their office space. All business-related printed matter must be disposed of using appropriate receptacles (such as waste bins designated for this purpose) or shredders.
- To ensure the confidentiality of and protect Computing Systems, Zuora may remotely delete data stored on a User's Computing System. This may include deleting data at the end of User's tenure or if a Computing System is reported lost, stolen, compromised or retired. In its sole discretion, Zuora may delete data, including professional or personal information or work-related data stored on a User's Computing System. Users should not store non-Zuora information (including pictures, files, documents, emails) on their Computing System.

6. COMPLIANCE

Users are required to understand and comply with this Policy along with any subsequent corporate directives regarding appropriate use of Computing Systems, regardless of form (signage, memo, electronic mail, etc.).

Any User found to have violated this Policy will be subject to discipline or similar action by Zuora. Human Resources will lead an investigation with the assistance of the Security Team to review the matter and determine appropriate next steps.

Zuora may take affirmative action against any User found to have violated this Policy, including suspension of privileges and in the most severe cases, termination for cause.

7. REPORTING

All Users are required to report instances of noncompliance with this Policy. If you notice activity that violates this Policy, email hr@zuora.com and security@zuora.com immediately with a description of the activity.

8. EXCEPTIONS

If a User believes that an exception should be made to this Policy, the User should describe the exception(s) (along with a reference to specific Policy sections) when completing the Acceptable Use Policy Acknowledgement Form. Any questions or comments should be sent to security@zuora.com.

9. ACKNOWLEDGEMENT FORM

All Users are required to review and acknowledge this Policy. After reviewing this Policy, please click the following link, complete the form, and submit: Acceptable Use Policy Acknowledgement Form. Additionally, please save a copy of this document for your future reference. The latest version of this document can be found here.

10. Zuora's Privacy Practices

To continue Zuora's established culture of openness, trust, integrity, Zuora has published a ZEO Privacy Notice. Refer to Zuora Policies page on the intranet site for additional details.