Acceptable Use Policy

Last revision date: 08/08/2023

ZUORA

Revision History

Version	Date	Change Log
1.0	4/13/2009	Initial Revision
2.0	5/20/2011	Conversion of policy to Confluence
3.0	8/8/2013	Move policy to Security Confluence Space
4.0	11/2/2015	Updated acceptable use policy statements and structure
5.0	6/30/2016	Annual Review - no changes needed.
6.0	6/7/2017	Updated 5.5.7 to include that users should not modify the hostname of their computers
7.0	6/21/2018	Annual review - no changes needed
8.0	5/29/2019	Annual review - no changes needed
8.1	7/20/2019	Added wording related to not using the same password across different platforms.

9.0	7/30/2021	Annual review - no changes needed
10.0	9/22/2022	Annual Review - no changes needed
10.1	08/08/2023	Annual Review - grammar + spelling cleanup

Table of Contents

1. Policy

Zuora's intention for publishing an Acceptable Use Policy is not to impose restrictions contrary to Zuora's established culture of openness, trust, and integrity. Zuora is committed to protecting customers, staff, and partners from illegal or damaging actions by individuals, either knowingly or unknowingly. Effective security is a team effort requiring the participation and support of every Zuora 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.

Users of Zuora's information systems require explicit approval and authorization from the owner of the technology/data/program, and the Security team.

2. Purpose

The purpose of this policy is to outline the acceptable use of computing facilities at Zuora. These guidelines are in place to ensure all Users (employees, contractors, consultants, and agents) use the computing facilities in an effective, safe, efficient, ethical and lawful manner. Inappropriate use of computing facilities exposes Zuora to risks including virus attacks, compromise of network systems and servers, and legal issues.

3. Scope and Audience

All (but not limited to) employees, contractors, consultants, and interns at Zuora, including subsidiaries and affiliated companies, must adhere to this policy. The scope of this policy includes the following critical technologies:

- Mobile devices
    - Laptops
    - Smartphones
    - Tablets
- Wireless networks
- Remote access/VPN
- Removable media
- Internet
- e-mail
- Office key cards

4. Roles and Responsibilities

- Security develops, reviews, and oversees the policy.
- Managers, in cooperation with Security, are required to train employees on policy and document issues with Policy compliance.
- IT oversees system integrity, monitors, and reports actions relating to computing facilities.
- HR conducts global coordination and is the custodian of relevant forms.
- Senior Executive Management conducts review and enforcement of policy.
- All employees, contractors, consultants, and interns (but not limited to) at Zuora, including all personnel affiliated with third parties are required to understand, acknowledge, and adhere to the terms of this policy.

5. Policy Directives

5.1 Acknowledgement Form

Users will sign the Acceptable Use Policy Acknowledgement Form, or another document, which states that the user has read and agrees to adhere to the terms and conditions of this policy.

5.2 General Use

Computing facilities and electronic communication systems, including voicemail, hardware and software used for e-mail, Internet access and Intranet access are the property of Zuora. All information, data and messages created, received, sent, or stored in these computing facilities and systems are, at all times, the property of Zuora.

5.3 Maintaining System Integrity

Zuora computing facilities shall be configured by the Zuora IT Department according to a platform build standard. Users shall not make changes to the platform standard, modify the hardware configuration, or modify the Operating System unless authorized by the IT Department. The user shall be responsible and liable for any and all direct or indirect damages to Zuora property as a result of such unauthorized changes. Default installations for personal computing facilities shall include:

- 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 and immediately report any faulty or non-existent instances of these tools to Security.

Users are responsible for protecting the computing facilities and related information assets of Zuora. Users are responsible for complying with the Zuora Information Security Policy, Password Policy, and any other accompanying policies as designated by Security. Users shall exercise reasonable care to protect mobile computing facilities while outside of Zuora premises. The same passwords should not be used across different platforms regardless if they are internal or external, work or person. For example, your Okta password, work GMAIL, and personal GMAIL should never be the same.

5.4 Monitoring

Zuora reserves the right to monitor computing facilities for appropriate use, and to review, control, audit, intercept, access and disclose all messages, files or data created, received or sent through the computing facilities, with or without notice to the user.

5.5 Unacceptable Use

5.5.1 General Requirements

- Users are responsible for exercising good judgment regarding appropriate use of Zuora resources in accordance with policies, procedures, and guidelines. Zuora resources may not be used for any unlawful or prohibited purpose.
- Users must report any incidents of possible misuse or violation of this Acceptable Use Policy to Human Resources (HR) via email, telephone, or in person.
- Users are prohibited from providing information about Zuora employees and customers (including, but not limited to lists containing names of employees), to parties outside of Zuora, except with prior authorization from customers, legal, or human resources (HR).

5.5.2 System Accounts and Access

- Users should not share their account(s), passwords, Security Tokens (i.e., google authenticator), or similar information or devices used for identification and authorization purposes.
- Users should not store or take offsite any customer data. (Refer to Information Security Policy).
- Users should not send unprotected sensitive customer data including Personally identifiable information (PII), Protected health information (PHI), and Primary Account Number (PAN) using end-user messaging technologies such as email, instant messaging, and chat.
- Users should not attempt to access any data, files, or programs that have not been formally authorized by an appropriate approver.

5.5.3 Software

- Users should not run or install a malicious program/software that may damage Zuora's assets. This includes, but is not limited to, programs known as computer viruses, Trojan horses, worms, and malware.
- Users should not use any P2P (Peer-2-Peer) file-sharing software for unauthorized download or that violate copyright laws (Kazaa, BitTorrent, Limewire, et al).
- Users should not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright and shall not otherwise use Zuora computing facilities to create, host, or transmit material which infringes copyright, trademark, patent, trade secret, or other proprietary rights of any other party.
- Users should not download, install, or run programs/software or utilities which reveal weaknesses in the security of a system unless required based on job responsibilities.
- Users should not use any unauthorized software or applications for the purposes of transmitting, processing, or storing of Zuora and or Zuora’s customer data.

5.5.4 Network Use

- Users should not use packet sniffing, packet flooding, spoofing, network scanning, denial of service, and forging routing information for malicious purposes unless required based on job responsibilities.
- Users should not connect unauthorized equipment or networks to any Zuora computing facilities. Connection of equipment to Zuora network requires the explicit review and authorization of the Security team.
- Users should not interfere with the normal operation of computers, terminals, peripherals, or networks.
- Users should not attempt to monitor or tamper with another user's electronic communications, read, copy, change or delete another user's files or software unless required based on job responsibilities.

5.5.5 Electronic Communications

- Users should not use Zuora's email address other than for business/professional purposes. All individuals are accountable for their actions on the internet and email systems.
- Users should not forge, misrepresent, obscure, or replace a user identity on any electronic communication to mislead the recipient about the sender.
- Users should not directly communicate with the press or in public forums. All direct public inquiries regarding Zuora's business needs to be routed to an authorized spokesperson.

5.5.6 Computing Facilities

- Users should not use Zuora computing facilities for commercial activity outside of legitimate Zuora business.
- Users should not send from/to/store on Zuora computing facilities any fraudulent, harassing, defamatory, offensive, indecent, or obscene messages. Spamming (unsolicited commercial email), chain letters or any other form of inappropriate mass mailing is strictly prohibited, internally or externally. Solicitations for religious or political causes or for personal financial gain are also specifically prohibited.

5.5.7 Computing Assets and Clear Desk

- Users should not modify the hostname of their company issued laptop.
- Users should not leave assigned Zuora assets (e.g., laptops) unsecured. Security measures should be taken when leaving laptops overnight in Zuora facilities/buildings such as placing in locked drawer or cabinet.
- Users should not leave confidential material on printers, photocopiers, or office space. All business-related printed matter must be disposed using confidential waste bins or shredders.

6. Compliance

Users shall comply with all corporate directives regarding appropriate use, regardless of form (signage, memo, electronic mail, etc).

Anyone found to have violated this policy is subject to action by the company. Human Resources will lead an investigation of the issue. Results of that investigation could lead to action being taken including suspension of privileges and in the most severe cases, termination for cause.

7. Reporting

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

8. Exceptions

Any exceptions to this AUP policy that is due to job responsibilities, the user should complete the Acceptable Use Policy Acknowledgement Form and provide description of the exception to the specific AUP policy sections. Any questions/comments should be sent to security@zuora.com.

Appendix A

Acceptable Use Policy - Acknowledgement Form

All (but not limited to) employees, contractors, consultants, and interns at Zuora are required to review and signoff of this policy.

To go to the signoff form, click here: Acceptable Use Policy Acknowledgement Form