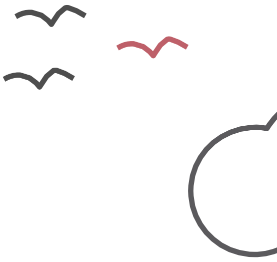
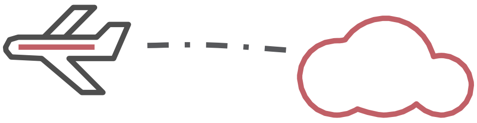
Information Security Policy

Last revision date: 09/08/2022





Program	Information Security	Status	Approved
Version	4.0	Version Date	September 08, 2022

Confidentiality

This document contains confidential Zuora information. This document is intended solely for use by internal Zuora personnel, Zuora business partners, Zuora customers, and Zuora prospective customers that have completed a non-disclosure agreement with Zuora.

Unauthorized use, reproduction, or distributions of this document, in whole or in part, is strictly prohibited.

Disclaimer

The information contained herein is believed to be accurate at the time of issue; no liability can be accepted for any inaccuracies. The reader is reminded that changes may have taken place since issue

ZUORA INFORMATION SECURITY POLICY

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Zuora’s relationship business management solution enables businesses around the world from startups to enterprises in any industry to launch and monetize subscription products and services. The evolving subscription economy brings new challenges to how organizations secure information and manage risk. Information management is an essential component of IT governance and a foundation for strong corporate governance. Information security must be an operating principal of an organization where documented policies, procedures, and standards are measured and evaluated against.

There are many frameworks for information security management. Zuora’s information security program is founded on the core principles for information security management defined in ISO/IEC 27002. In addition to ISO 27002, Zuora’s Information Security Policy provides a flexible framework that addresses the needs of ISO 27001, ISO 27018, ISO 27701, PCI DSS, SOC 1, SOC 2, HIPAA, and international privacy regulations. This policy outlines specific information security requirements for the following areas:

- Organizational security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- Systems acquisition, development, and maintenance
- Supplier relationships
- Incident management security
- Business continuity security
- Compliance

This policy applies to Zuora computer systems, networks, and information assets. The intended audience for this policy includes all Zuora staff, including employees (full-time, contractors, or temporary staff) and all applicable partners that may access any Zuora resources. The intended audience is responsible for applying the principles of information security in their role at Zuora and must adhere to the policies and instructions in this document.

INFORMATION SECURITY POLICY

Security Statement

Zuora is committed to safeguarding the confidentiality, integrity, and availability of all physical and electronic information assets of the Company to ensure that regulatory, operational, and contractual requirements are fulfilled. Zuora management takes information security seriously and this policy provides the baseline and direction for managing information systems and their security. All Zuora employees, contractors, vendors, and business partners must demonstrate support for, and commitment to, information security practices defined in this policy. The overall goals of information security at Zuora are the following:

- Ensure compliance with laws, regulations, and guidelines.
- Establish controls for protecting Zuora's information and information systems against theft, abuse, and loss.
- Establish controls for protecting Zuora's customer information.
- Ensure that Zuora can continue the operation of the services in the event of a major security incident.
- Ensure the confidentiality and privacy of personal data.
- Comply with information security requirements of the following standards and regulations:
  - International Organization for Standards (ISO) 27001
  - Payment Card Industry Data Security Standards (PCI DSS) Level 1
  - Service Organization Control (SOC) Trust Services Principals (SOC 2)
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Health Information Technology for Economic and Clinical Health Act (HITECH)
  - General Data Protection Regulation (GDPR) (EU 2016/679)
  - California Consumer Privacy Act (CCPA)

This policy shall be reviewed at least annually. During this review the contents of this policy must be updated as needed to reflect changes to business objectives or the risk environment.

Any deviations and exceptions from the requirements outlined in this Information Security Policy or supporting security procedures must be formally submitted to Zuora's Security and Compliance team with a business justification for the deviation from the policy. All deviations and exceptions require formal approval by the Chief Security Officer.

Security Strategy

The purpose of this policy is to define Zuora policy baseline and direction, and to demonstrate support for, and commitment to, information security through the issue and maintenance of an Information Security Policy across the organization. The remainder of this document contains Zuora policies for information security.

In addition to this Information Security Policy Zuora has developed a number of underlying policies, procedures, and standards detailing how aspects of this policy are to be implemented for specific parts of the organization. These documents should be used in conjunction with this policy when evaluating specific information security practices at Zuora Information Security includes a number of principles, including the following:

CONFIDENTIALITY

Confidentiality is the protection of information within systems so that unauthorized individuals, resources, and processes cannot access that information. That is, confidentiality means the system does not allow information to be disclosed to anyone who is not authorized to access it. Privacy issues and regulations such as California S.B 1386, FRCP E-Discovery, EU General Data Protection Regulation 2016/679, and the California Consumer Privacy Act emphasize the importance of confidentiality on protecting and processing personal information and records maintained in automated information systems.

Confidentiality should be well defined, and procedures for maintaining confidentiality should be carefully implemented. Crucial aspects of confidentiality are user identification, authentication, and authorization.

Confidentiality can be compromised in several ways. The following are some of the most common encountered threats to information confidentiality:

- Hackers: someone who bypasses the system's access controls by taking advantage of security weaknesses that the system's developers have left in the system. In addition, many hackers are adept at discovering the passwords of authorized users who choose passwords that are easy to guess. The activities of hackers represent serious threats to the confidentiality of information in computer systems.
- Masquerading: an attempt to gain access to system by posing as an authorized user.
- Unauthorized user activity: when users gain access to files they are not authorized to access. Weak access controls often enable such compromise confidential information.
- Networks: present a special confidentiality threat because data following through networks can be viewed at any node of the network. This is particularly significant because unencrypted user IDs and passwords are subject to compromise by a "sniffer". Any confidential information not intended for viewing by everyone should be protected by encryption techniques.
- Malicious software: software that have been programmed to copy confidential files to unprotected area of the system or other resources when they are unknowingly execute by the users who have authorized to access those files
- Social engineering: a human interaction that involves tricking an authorized user to break security procedures.

INTEGRITY

Integrity is the protection of systems information or processes from intentional or accidental unauthorized changes. Like confidentiality, integrity can be compromised by hackers, masqueraders, unauthorized user activity, networks, and malicious codes because each of these threats can lead to unauthorized change to data or programs. Three basic principles are used to establish integrity controls:

- Separation of duties
- Granting access on a need-to-know/least privilege basis
- Rotation of duties

AVAILABILITY

Availability is the assurance that a computer system is accessible by authorized users when needed.

Two facets of availability are typically discussed:

- Denial of service
- Loss of data processing capabilities as a result of nature disasters or human actions.

Denial of service usually refers to user or intruder actions that tie up the computing services in a way that renders the system unusable by authorized users. Loss of data processing capabilities because of nature disasters or human actions is more common. Such loses are countered by contingency planning which provides an alternative means of processing, therefore ensure availability. Physical, operational, and administrative controls are important aspects of security initiatives that address availability.

PRIVACY

Information privacy is the right to have some control over how your personal information is collected and used.

Zuora is committed to protecting personal data and has in place appropriate data security measures that meet industry standards. We regularly review and make enhancements to our processes, products, documentation, and contracts to help support ours and our customers' compliance for the processing of personal data.

Zuora's comprehensive data protection and security program is designed to systematically confirm that our SaaS Service meets specific privacy requirements set forth by various regulations (e.g., GDPR, CCPA), focused specifically on the personal data of our customers.

ROLES AND RESPONSIBILITIES

Zuora executives and directors have the overall responsibility for managing Zuora’s risks in an effective and satisfactory manner in accordance with current laws, regulations, and contracts.

Owner of the Security Policy

The SVP of Software Engineering is the owner of this Information Security Policy. The SVP of Software Engineering has delegated the responsibility for security-related documentation to the Chief Information Security Officer (CISO). All policy changes must be approved and signed by the CISO.

Chief Information Security Officer

Zuora’s CISO has overall responsibility for managing information security at Zuora, including information security of the Zuora services provided to customers and internal corporate systems utilized by Zuora to conduct business.

The CISO is responsible for overseeing all aspects of information security, including but not limited to the following:

- Creating and distributing security policies and procedures.
- Creating and distributing privacy policies and reviewing Zuora's compliance with privacy commitments.
- Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel.
- Creating and distributing security incident response and escalation procedures that include:
  - roles, responsibilities, and communication
  - coverage and responses for all critical system components
  - notification, at a minimum, of credit card associations and acquirers
  - strategy for business continuity post compromise
  - reference or inclusion of incident response procedures from card associations
  - analysis of legal requirements for reporting compromises (for example, per California bill 1386)
- Annual penetration testing
- Designation of personnel to monitor for intrusion detection, intrusion prevention, and file integrity monitoring alerts on a 24/7 basis
- Developing, implementing, and monitoring security awareness and privacy training on a continual basis
- A process for evolving the incident response plan according to lessons learned and in response to industry developments
- Maintaining a formal security awareness program for all employees that provides multiple methods of communicating awareness and educating employees (for example: posters, emails, meetings)

- Generate security logs and follow-up on exceptions identified.

The Information Technology Office (or equivalent) shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS (for example, user account maintenance procedures, and log review procedures).

Security Oversight Committee

The CISO has established the Security Oversight Committee (SOC) consisting of representative's form various departments to drive security initiatives at Zuora. The formation of Zuora SOC is a result of an executive mandate to reinforce and strengthen the information security organization and infrastructure. The membership of the SOC is comprised of representatives from Legal, Engineering, Product, IT, Technical Operations, and Security.

The SOC also provides a forum within which to share knowledge and technology and address global security issues. The SOC's primary goals are to:

- To raise information security awareness
- To develop and review risk assessments and risk rankings at Zuora.
- To protect Zuora systems and critical information assets
- To collect and report information security metrics

Security and Compliance Team

Members of the Security and Compliance team are responsible for executing:

- Risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.
- The vulnerability management function shall be responsible for carrying out:
  - Running internal and external network vulnerability scans at least quarterly and after any significant changes in the network or cardholder data environment
  - Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification
  - Use intrusion detection systems and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment
- Managing the compliance program to meet quarterly, biannually, and annual objectives
- Manage employee participation in the security awareness program
- Provide recommendations and guidance on technical security
- Ensuring and tracking that employees acknowledge in writing that they have read and understand the company's Acceptable Use Policy, which includes the company's Information Security Policy
- Tracking employee compliance with the Acceptable Use Policy
- Create user awareness by conducting simulated phishing campaigns
- Vendor oversight and continuous monitoring
- Managing data privacy

System Acquisition and Ownership

The Chief Information Officer (CIO) is responsible for purchasing requirements, development and maintenance of information and related information systems. All systems and all types of information must have a defined owner. The system owner must define which users or user groups are allowed access to the information and what authorized use of this information consists of. The system ownership shall be described in a separate document.

System Administrator

System administrators are persons administrating Zuora's information systems and the information entrusted to the company by other parties. Each type of information and system may have one or more dedicated system administrators. These are responsible for protecting the information, including implementing systems for access control to safeguard confidentiality, and carry out backup procedures to ensure that critical information is not lost. They will further implement, run, and maintain the security systems in accordance with the Information Security Policy.

System and Application Administrators shall:

- Monitor and analyze security alerts and information and distribute to appropriate personnel
- Administer user accounts and manage authentication
- Monitor and control all access to data
- Maintain a list of connected entities
- Perform due diligence prior to connecting an entity, with supporting documentation
- Verify that the entity is PCI-DSS compliant, with supporting documentation
- Establish a documented procedure for connecting and disconnecting entities
- Retain audit logs for at least one year

Human Resources

Human Resources is responsible for the on-boarding and off-boarding of employees and contractors. This includes, but is not limited to, the following:

- Develop and maintain company organization charts to communicate key areas of authority, responsibility, and lines of reporting.
- Maintain job descriptions with defined skills, responsibilities, and knowledge levels required for particular jobs.
- Screen potential employees to minimize the risk of attacks from internal sources.
- Ensure that background checks are performed for employees
- Ensure appropriate employment agreements are signed by all employees and contractors

Legal

Legal will ensure that for service providers with whom cardholder information is shared:

- Contracts require adherence to PCI-DSS by the service provider
- Contracts include acknowledgement or responsibility for the security of cardholder data by the service provider

Users

Employees, contractors, and consultants are responsible for getting acquainted and complying with Zuora's IT regulations. Questions regarding the administration of various types of information should be posed to the system owner of the relevant information, or to the system administrator.

Consultants and Partners

Contractual partners and contracted consultants must sign a confidentiality agreement prior to accessing sensitive information. The System owner is responsible for ensuring that this is implemented.

Information Security Management Team

The members of the Information Security Management Team include:

Role	Team Member(s)
Chief Product & Engineering Officer	[redacted]
Chief Information Security Officer	[redacted]
Chief Human Resources Officer	[redacted]
SVP General Counsel and Secretary	[redacted]
VP Technical Operations	[redacted]

PRINCIPLES FOR INFORMATION SECURITY AT ZUORA

Risk Management

RISK ASSESSMENT AND MANAGEMENT

Risk management is an oversight process undertaken on a continuous basis. This process involves risk identification, assessment, control, and mitigation. The scope of risk management embraces a broad horizon, which incorporates risk anticipation and preclusion. To quantify risks, it is necessary to assess vulnerabilities, threats, the cost of required security measures, and the impacts of the threats if unmitigated.

Zuora performs an overall annual risk assessment that formally documents the identified threats, vulnerabilities, likelihood, and potential impacts to the organization. The results of this risk assessment are presented to management.

Zuora’s information security risk management framework includes the following elements:

- Identify the information assets of Zuora.
- Prioritize information assets according to their worth to Zuora.
- Identify, analyze, quantify, and mitigate technology risks.
- Implement appropriate security policies and measures to safeguard the integrity and reliability of information assets.
- Protect information assets against external and internal threats.
- Maintain a strong capability to detect and respond to attacks and suspicious activities on its networks or systems.

RISK MANAGEMENT RESPONSIBILITY

Overall risk management policies are the responsibility of Zuora senior management. Information risks and security threats are not technical issues but business issues. High-level risk management strategy is an oversight process applied on a continuous basis. Zuora should develop risk management processes according to risk acceptance levels, security profiles, and Zuora governance culture. Zuora should also develop rapid response contingency plans in order to be prepared for new risks and new threats, which may arise unexpectedly.

Risk management is the responsibility of the security and compliance team at Zuora. The security and compliance team conducts periodic risk assessments and works with departments across the organization to prioritize and mitigate risks identified in the assessment. It is the responsibility of the security and compliance team to accurately communicate the severity of identified risks to the organization so that business owners can determine the appropriate course of action for the company.

Information Security Policy

The CISO shall ensure that the Information Security Policy, as well as security procedures and standards, are utilized and acted upon. Additionally, the CISO must ensure that the availability of sufficient training and information material for all employees, contractors, and partners in order to enable users to protect Zuora’s data and information systems.

The Information Security Policy shall be reviewed and updated annually or when business needs change, in accordance with the following standards and regulations:

- □ ISO/IEC 27001
- □ PCI DSS
- □ SOC 1
- □ SOC 2
- □ HIPAA/HITECH

All significant changes to Zuora’s activities, and other external changes related to the threat level, should results in a revision to the policy and supporting procedures and standards relevant to information security.

Classification and Control of Assets

Information and infrastructure should be classified according to security level and access control. “Assets” include both information assets and physical assets. Zuora shall carry out periodic risk analysis in order to classify information based on how critical it is for operations. Sensitive documents should be clearly marked and secured to maintain security in accordance with the criticality of such information.

To assist in the appropriate handling of information, a sensitivity classification hierarchy should be used throughout Zuora. This hierarchy provides a shorthand way of referring to sensitivity and can be used to simplify information security decisions and minimize information security costs. One important intention of a sensitivity classification system is to provide consistent handling of the information, no matter what form it takes, no matter where it goes, and no matter who possesses it. For this reason, it is important to maintain the labels reflecting sensitivity classification categories.

Zuora uses four classification categories:

- Customer Confidential Information
- Zuora Confidential Information
- Internal Use Only Information
- Public Information

CUSTOMER CONFIDENTIAL INFORMATION

Customer confidential information is any information a customer submits to Zuora through Zuora’s production tenants and non-production environments for the purposes of allowing Zuora to perform activities that the customer contracts Zuora to perform. Any customer data that Zuora stores, processes, creates, or receives is classified as customer confidential data.

Access to customer data is granted and based on those individuals required to complete their job functions/responsibilities. Access should be restricted to a limited set of users. Distribution of customer confidential data is highly restricted and cannot be shared outside of Zuora without authorization from the customer and Legal's approval. To reiterate this sensitivity and confidentiality of customer data, annual security and privacy training is performed, in addition to the monitoring that is performed to data extracts. Some examples of Customer Confidential Information include: Personally Identifiable Information (PII), Cardholder data information, or Protected Health Information (PHI).

ZUORA CONFIDENTIAL INFORMATION

Confidential information is non-public information, whether written or oral, visual or machine –readable form, provided by Zuora (including its employees and contractors) to a third party. Use of Zuora confidential information by third parties requires the receiving party to assume non-disclosing obligations in a duty executed agreement.

Access to Zuora confidential information is restricted to employees or contractors on a need-to-know basis. Distribution of Zuora confidential information to a third party requires the party to be bound by appropriate confidentiality obligations. Examples of confidential information include: Financial information, Employee information, Customer list, Corporate strategic plans, Intellectual property, Audit findings, and Vendor confidential information such as pricing, proposals.

INTERNAL USE ONLY INFORMATION

Internal use information is any information that is proprietary or produced only for use by employees of Zuora who have legitimate purpose to access such data.

Access to Internal Use Only Information is restricted to employees or contractors of Zuora. Internal Use Only Information cannot be shared or distributed to external individuals. Examples include: Corporate policies, Standard Operating Procedures, Internal email communications, Technical documentation, such as system configurations and network diagrams, All Company-developed software code, whether used internally or sold to clients.

PUBLIC INFORMATION

This classification covers information that can be disclosed to any person inside or outside Zuora. Although security mechanisms are not needed to control disclosure and dissemination, they are still required to protect against unauthorized modification and destruction of information. Examples include: press releases approved for distribution to media, marketing materials approved for distribution, financial reports required by regulatory authorities, newsletters for external transmission, publicly posted information on products. Disclosure of Zuora information to the public requires the existence of this label, the specific permission of the information owner, or long-standing practice of publicly distributing this information.

Human Resource Security

Personnel Security refers to the practices, technologies and/or services used to ensure that personnel security safeguards are applied appropriately to those personnel working for, or on behalf, of Zuora. Part of personnel security includes defining the roles and responsibilities for or employees and contractors and ensuring that new hires have the appropriate skill sets in order to meet the job requirement. Role and responsibility definition are owned and maintained by Human Resources, with updates made regularly.

PRIOR TO EMPLOYMENT

The following activities must be conducted on staff prior to employment:

- A background check is to be carried out of all appointees to positions at Zuora according to relevant laws and regulations. The background check will include the following or equivalent, as legally allowed per country:
    - Social Security Number Trace
    - County Court Criminal Conviction
    - CrimeSweep National Search
    - Driver's License Abstract
    - Employment Verification
- A mutual non-disclosure agreement (MNDA) should be signed by employees, contractors or others who may gain access to sensitive and/or internal information.

DURING EMPLOYMENT

While employed at Zuora employees must sign and follow the requirements of Zuora’s Acceptable Use Policy, which includes this Information Security Policy.

All employees and third-party users, including but not limited to, interns and contractors, should receive annual security awareness and privacy training and education on updated Information Security Policy and procedures. The training requirements may vary.

Breaches of the Information Security Policy and accompanying guidelines will result in disciplinary action that may include termination. Zuora's information, information systems, and other assets should only be utilized for their intended purpose. Necessary private usage is permitted. Employee and third parties are prohibited from copying Zuora data to personal devices, except for company email permitted on personal mobile devices that have been enrolled with IT using Exchange integration for management. At no time may an employee connect a personal device to Zuora’s production systems and networks. Zuora Security must approve all other use in advance.

TERMINATION OR CHANGE OF EMPLOYMENT

Zuora requires all access be revoked for individuals that leave Zuora immediately upon termination.

Terminations must be kept confidential and notice of a planned termination must never be shared with the employee being terminated. In the event on an involuntary termination, documentation of the termination should not be stored in the Zuora helpdesk, unless the terminated individual can logically separate it from viewing. Zuora currently uses a Salesforce-based solution as their IT ticketing system, with access restricted to Human Resources, IT, and Security departments. In the event that a termination involves a member of Human Resources, IT, or Security the termination process will be communicated directly between Human Resources and IT individuals performing the termination activity as to prevent the terminated employee from gaining knowledge of the termination.

Physical Security of Information Systems

Physical and environmental security refers to those practices, technologies, and/or services used to ensure that physical security safeguards are applied. Physical security safeguards take into account include:

- The physical facility housing the information resources;
- The general operating location; and
- The support facilities that underpin the operation of the information systems.

Physical security safeguards provide a first line of defense for information resources against physical damage, physical tampering, physical theft, unauthorized disclosure of information, loss of control over system integrity, and interruption to computer services.

Zuora's IaaS providers limit physical access to information resources and the facilities in which they are located while taking reasonable steps to ensure that properly authorized service provider employees only have access to its facilities. Zuora ensures, where possible, that information resources are located in areas where physical access can be controlled in order to minimize the risk of unauthorized access. Zuora takes reasonable steps to ensure that the level of protection provided for the information resources, as well as the facilities in which they are housed, is commensurate with that of the identified threats and risks. Zuora will establish the following policies and procedures as part of its commitment to complying with this standard.

Mission critical system facilities must be located in a secure location that is locked and restricted to authorized personnel only.

- Access to "critical" computer hardware, wiring, displays and networks should be controlled by rules of least privilege.
- System configurations (i.e., hardware, wiring, displays, and networks) of "critical" systems should be documented. Installations and changes to those physical configurations should be governed by a formal change management process.
- A system of monitoring and auditing physical access to "critical" computer hardware, wiring, displays and networks should be implemented (e.g., badges, cameras, access logs).
- Unrestricted access to the central computer facilities will be confined to designated staff whose job classification requires access to that particular area/equipment. Restricted access may be given to other staff where there is a specific job function need for such access.
- Third party support agencies will only be given access through specific authorization.
- All secure areas will have an entry log which staff and visitors must use.
- Regular reviews of who can access these secure areas should be undertaken.

Technical Operations and Communications Management

Technical Operations refers to activities done to run the systems that power the Zuora services. This includes both system administration and tasks external to the system that support its operation (e.g., maintaining documentation). It does not include system planning or design. Support and operations are routine activities that enable the production systems to function correctly. These include fixing software or hardware problems, loading and maintaining software, and helping users resolve problems.

The important security considerations within some of the major categories of support and operations are:

- User support,
- Software support,
- Configuration management,
- Backups,
- Media controls,
- Documentation,
- Maintenance.

This section addresses the support and operations activities directly related to security. Every control discussed in this document relies, in one way or another, on computer system support and operations.

CRITICAL EMPLOYEE-FACING TECHNOLOGIES

For critical employee-facing production technologies, departmental procedures shall require:

- Explicit management approval to use the technology
- That all device use is authenticated with username and password or other authentication item (for example, token)
- A list of all devices and personnel authorized to use the devices
- Labeling of devices with owner, contact information, and purpose
- Automatic disconnect of modem sessions after 15 minutes of inactivity
- Activation of modems used by vendors only when needed by vendors, with immediate deactivation after use

OPERATIONAL PROCEDURES AND AREAS OF RESPONSIBILITY

Zuora’s procurement department must approve purchase and installation of IT equipment. The engineering, security, legal, and finance departments at Zuora must approve purchase and installation of software for IT equipment. The Technical Operations department should ensure documentation of the IT systems according to Zuora's standards; this includes security and system hardening documentation. Changes in IT systems should only be implemented if well founded from a business and security standpoint.

Before a new IT system is put in production, plans and risk assessments should be in place to avoid errors. Additionally, routines for monitoring and managing unforeseen problems should be in place.

Duties and responsibilities should be separated in a manner reducing the possibility of unauthorized or unforeseen abuse of Zuora's assets. Development, testing, and maintenance should be separated from operations in order to reduce the risk of unauthorized access or changes, and in order to reduce the risk of error conditions.

THIRD PARTY SERVICES

All contracts regarding outsourced IT systems should include:

- Requirements for reporting security incidents from third parties,
- Information security requirements, including confidentiality, integrity, and availability,
- A description of the agreed security level,
- A description of how Zuora may ensure that third parties are fulfilling their contracts,
- A description of Zuora's right to audit third parties.

USER SUPPORT

Zuora has established a group, which is responsible for assisting with end-user support. In general, system support and operations staff need to be able to identify security problems, respond appropriately, and inform appropriate individuals. A wide range of possible security problems could exist on any of the following: custom applications, off-the-shelf products, and software or hardware issues. The scope of their work is communicated to customers through the Knowledge Center:

> *https://knowledgecenter.zuora.com/BB_Introducing_Z_Business/Policies/Global_Support_Scope.*

Based on Zuora's policy, Customers are responsible for managing their data and making any updates as necessary. In the case that an update cannot be made, a Support Ticket should be created.

As part of their function, Zuora’s user support organization should be able to recognize which problems (brought to their attention by users) are security related. For example, users' inability to log onto a computer system may result from the disabling of their accounts due to too many failed access attempts. This could indicate the presence of hackers trying to guess users' passwords.

SOFTWARE SUPPORT

Software is the heart of our computer operations. Therefore, it is essential that software function correctly and be protected from corruption. There are many elements of software support.

One way to protect software from corruption is to control what software is used on a system. If users or systems personnel can load and execute any software on a system, the system is more vulnerable to viruses, to unexpected software interactions, and to software that may subvert or bypass security controls. One method of controlling software is to inspect or test software before it is loaded. This can apply to new software packages, to upgrades, to off-the-shelf products, or to custom software, as deemed appropriate. In addition to controlling the loading and execution of new software, we should also give care to the configuration and use of powerful system utilities. System utilities can compromise the integrity of operating systems and logical access controls

A second element in software support can be to ensure that software has not been modified without proper authorization. This involves the protection of software and backup copies. This can be done with a combination of logical and physical access controls.

CONTROLS AGAINST MALICIOUS SOFTWARE

As part of defense-in-depth strategy, Zuora deploys malicious software checking programs on all Windows servers and on individual end-user systems for all Zuora employees. Anti-Virus / Endpoint Detection & Response (EDR) software is installed on all systems affected by viruses, trojans, and malicious software.

Employees are prohibited from bypassing or disabling such software unless properly authorized to do so by the security team. Antivirus software examines all electronic mail attachments, downloads, and electronic media to confirm they do not contain malicious software. Zuora subscribes to updates for all malicious software checking programs, including anti-virus software.

Zuora will deploy Anti-Virus software on all Windows servers. Anti-Virus software will be configured to automatically update virus definitions, perform real time protection, perform weekly system scans, not exclude any system file types or locations, and remove quarantined files after three months. All Microsoft anti-malware logs will be forwarded to Zuora's log repository solution where they are retained for at least one year.

All individual end-user laptops are protected with Anti-Virus/EDR, computers are managed by a central management client and routinely reviewed by IT for triage.

BACKUPS

Support and operations personnel perform backups of software and data, which is critical to contingency planning. Frequency of backups will depend upon how often data changes and how important those changes are. Program managers should be consulted to determine what backup schedule is appropriate. Also, as a safety measure, it is useful to test that backup copies are actually usable. Finally, backups should be stored securely, as appropriate.

Data should be held on a network directory where possible, to ensure routine backup processes capture the data. Data should be protected by clearly defined and controlled back-up procedures, which will generate data for archiving and contingency recovery purposes. Information Technology and all other systems managers should produce written backup instructions for each system under their management. The backup copies should be clearly labelled and held in a secure area where applicable. Procedures should be in place to recover to a usable point after restart of this backup. A cyclical system, whereby several generations of backup are kept, is recommended.

- Archived and recovery data should be accorded the same security as production data and should be held separately, preferably at an off-site location or geographically dispersed region.
- Archived data is information, which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes.
- Recovery data should be sufficient to provide an adequate level of service and

recovery time in the event of an emergency and should be regularly tested.

- To ensure that, in an emergency, the backup data is sufficient and accurate, it should be regularly tested. This can be done by automatically comparing it with the live data immediately after the backup is taken and by using the backup data in regular tests of the contingency plan.

Recovery data should be used only with the formal permission of the data owner or as defined in the documented contingency plan for the system. If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the backup data. This aims to ensure that back-up data is not corrupted in addition to the live data.

DATA RETENTION

To ensure all types of card holder are covered, Zuora identifies the following unique types of cardholder data being used by the business:

- Active tenants
- Active accounts
- Inactive accounts
- Cancelled Accounts
- Inactive tenants
- Encrypted data backup
- Cardholder data in written form
- Cardholder in digital form

Cardholder data used by active accounts may be kept in the system for as long as it is utilized by the customer or end user for an active tenant. Cardholder data utilized for recurring transactions will be retained by our third-party outsourcing agent, or as required by Zuora in an encrypted format for processing future transactions. For inactive and cancelled accounts, cardholder data may be retained in the system in a secure encrypted format as long as the tenant is active in the system. Cardholder data for inactive tenants is deleted after a specified duration.

Cardholder data should not be stored in written format in any way. Any card holder data written temporarily on paper for processing purposes or accidentally must be discarded either by processing it through a shredder and disposing them securely into multiple different trash locations, or by disposing it within one of our secured trash bins.

All system audit logs related for PCI Cardholder Data Environment (CDE) systems must be retained for a minimum of one (1) year in a secure central log repository and have a minimum of three (3) months of audit log information available for immediate analysis. To meet this requirement, all clients within scope shall be configured to send critical audit logs to the central log server for retention and analysis.

DISPOSAL REQUIREMENTS

All confidential or sensitive electronic data, when no longer needed for legal, regulatory, or business requirements must be removed from Zuora systems using an approved method documented in this policy. This requirement includes all data stored in systems, temporary files, or contained on storage media.

All confidential or sensitive hardcopy data, when no longer needed for legal, regulatory, or business requirements must be disposed by using an approved method documented within the Data Retention and Destruction Policy.

DISPOSAL AND REUSE PROCESS

Media containing confidential or sensitive card holder data that should no longer be retained must be disposed of in a secure and safe manner. Before computer or communications equipment can be sent to a vendor for trade-in, servicing, or disposal, all confidential or sensitive information must be destroyed or removed. Outsourced destruction of media containing confidential or sensitive information must use a bonded Disposal Vendor that provides a “Certificate of Destruction.”

If electronic media has ever stored cardholder, ePHI, Personally Identifiable Information (PII), or customer data then it must be securely erased prior to repurposing in a manner that prevents previously stored data from being accessed and reused. Note cardholder, ePHI, PII, or customer data should never be stored on removable media. Reuse activities should only be arranged through Information Technology Department who will arrange for disks to be wiped according to Zuora’s Media Handling Policy.

NETWORK ADMINISTRATION

Zuora’s IT department has overall responsibility for protecting Zuora’s corporate networks and Zuora’s Technical Operations department has overall responsibility for protection Zuora’s production networks. Each department is tasked with maintaining an inventory of all equipment connected to Zuora’s wired networks.

All access to production networks must be logged in a centralized logging solution. To meet objectives for network security, the following should be done:

- Security standards shall be established to set requirements for physical or virtual network devices
- Physical or Virtual Network devices must be configured according to defined security standards
- Network diagrams of critical production network environment must be maintained and kept up to date

MANAGEMENT OF STORAGE MEDIA

Media controls include a variety of measures to provide physical and environmental protection and accountability for tapes, diskettes, printouts, and other media. From a security perspective, media controls should be designed to prevent the loss of confidentiality, integrity, or availability of information, including data or software, when stored outside the system. This can include storage of information before it is input to the system and after it is output. Zuora’s Technical Operations and IT department must maintain a record of the movements of hardware and electronic media and any person responsible.

Media Labelling

Controlling media may require some form of physical labelling. The labels can be used to identify media with special handling instructions, to locate needed information, or to log media (e.g., with serial/control numbers or bar codes) to support accountability. Identification is often by colored labels on diskettes or tapes or banner pages on printouts.

Media Logging

The logging of media is used to support accountability. Logs can include control numbers (or other tracking data), the times and dates of transfers, names and signatures of individuals involved, and other relevant information. Periodic spot checks or audits may be conducted to determine that no controlled items have been lost and that all are in the custody of individuals named in control logs. Automated media tracking systems may be helpful for maintaining inventories of tape and disk libraries.

Media Transmittal

Media control may be transferred both within the organization and to outside elements. Possibilities for securing such transmittal include sealed and marked envelopes, authorized messenger or courier, or U.S. certified or registered mail.

MEDIA Disposition

When media is disposed of, it may be important to ensure that information is not improperly disclosed. This applies both to media that is external to a computer system (such as a diskette) and to media inside a computer system, such as a hard disk. As well, it also applies to hard-copy materials (such as paper reports). The process of removing information from media is called sanitization.

Three techniques are commonly used for media sanitization: overwriting, degaussing, and physical destruction. Overwriting is an effective method for clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination) onto the media.

Common practice is to overwrite the media three times. Overwriting should not be confused with merely deleting the pointer to a file (which typically happens when a delete command is used).

Overwriting requires that the media be in working order. Degaussing is a method to magnetically erase data from magnetic media. Two types of degassers exist: strong permanent magnets and electric degassers. The final method of sanitization is physical destruction of hard-copy materials. This is be accomplished by cross-cut shredding, incineration, or pulping such that there is reasonable assurance the hard-copy materials cannot be reconstructed or through the use of Zuora’s shred bins, which are placed sporadically throughout the main offices.

Transmission of Information

Information exchanged across public networks in connection with e-commerce, should be protected against fraud, contractual discrepancies, unauthorized access, and changes. The Technical Operations and Security departments should ensure that Zuora's services are adequately protected against unauthorized access.

Users shall not send unprotected sensitive customer data including PII, ePHI, and Cardholder Data (CHD) by end-user messaging technologies such as e-mail, instant messaging, and chat. Zuora has develop a secure file transfer process to transfer sensitive data, such as CHD. Please contact security@zuora.com or migration@zuora.com or support@zuora.com for more information on this process.

When required to send sensitive data such as CHD over end-user messaging technologies, please 1) obtain approval from Security (security@zuora.com), and 2) transmit such data using strong cryptography. This means data is transferred with security strength equal or greater than the following procedure:

- All data transfers shall be sent using an encrypted transfer protocol such as SSH, HTTPS, FTPS, or protocols leveraging updated TLS protocols
- All files must be encrypted with strong symmetric or asymmetric encryption before transmitting.
- Symmetric encryption of 128-bit security strength or higher. For example, AES-256
- Asymmetric encryption of 128-bit security strength or higher. For example, RSA 4096 bit or higher
- Symmetric encryption keys used for encryption of files must be sent over a separate channel from the channel used for transferring file. For example, over a phone call, in person, or using SMS text.
- Asymmetric encryption keys must be kept secured and protected from unauthorized access.

Display of Cardholder Data

Credit card numbers must be masked when displayed in any Zuora application. The maximum numbers of digits that can be shown are the first six and last four digits of a credit card number. As a practice Zuora only permits the last four digits of credit card digits. To achieve this Zuora will create a redacted credit card field in the Zuora database. This field is populated by an automated process that replaces all but the last four digits with an asterisk (e.g., ************1234). The redacted credit card number is called upon when the Zuora UI needs to display a credit card number for a customer. Non-redacted credit card numbers must be stored in an encrypted format and not displayed through the Zuora UI.

Zuora does not allow any roles access to display full CHD. No UI in the Zuora application displays full CHD. All roles at Zuora only see masked PAN.

Security Awareness and Privacy Education

The purpose of computer security awareness and privacy education is to enhance security by:

- Improving awareness of the need to protect system resources;
- Developing skills and knowledge so computer users can perform their jobs more securely, and
- Building in-depth knowledge, as needed, to design, implements, or operate security programs for organizations and systems.

An awareness program must be developed and maintained, with training taking place at least annually or, in the case of a new employee, contractor, or intern, within one (1) month of four (4) weeks, whichever is longer, of the person’s new hire date.

Monitoring

Security monitoring is an ongoing activity that looks for vulnerabilities and security problems. Many of the methods are similar to those used for audits, but are done more regularly or, for some automated tools, in real time.

AUTOMATIC TOOLS

Several types of automated tools monitor a system for security problems. Some examples follow:

- Automated tools can be used to help find a variety of threats and vulnerabilities, such as improper access controls or access control configurations, weak passwords, lack of integrity of the system software, or not using all relevant software updates and patches. These tools are often very successful at finding vulnerabilities and are sometimes used by hackers to break into systems. Not taking advantage of these tools puts system administrators at a disadvantage. Many of the tools are simple to use; however, some programs (such as access-control auditing tools for large mainframe systems) require specialized skill to use and interpret.
- Virus scanners are a popular means of checking for virus infections. These programs test for the presence of viruses in executable program files.
- Check summing presumes that program files should not change between updates. They work by generating a mathematical value based on the contents of a particular file. When the integrity of the file is to be verified, the checksum is generated on the current file and compared with the previously generated value. If the two values are equal, the integrity of the file is verified. Program check summing can detect viruses, Trojan horses, accidental changes to files caused by hardware failures, and other changes to files. However, they may be subject to covert replacement by a system intruder. Digital signatures can also be used.
- Password crackers check passwords against a dictionary (either a “regular” dictionary or a specialized one with easy-to-guess passwords) and check if passwords are common permutations of the user ID. Examples of special dictionary entries could be the names of regional sports teams and stars; common permutations could be the user ID spelled backwards.

- Integrity verification programs can be used by such applications to look for evidence of data tampering, errors, and omissions. Techniques include consistency and reasonableness checks and validation during data entry and processing. These techniques can check data elements, as input or as processed, against expected values or ranges of values; analyze transactions for proper flow, sequencing, and authorization; or examine data elements for expected relationships. These programs comprise a very important set of processes because they can be used to convince people that, if they do what they should not do, accidentally or intentionally, they will be caught. Many of these programs rely upon logging of individual user activities.
- Intrusion detectors analyze the system audit trail, especially log-ons, connections, operating system calls, and various command parameters, for activity that could represent unauthorized activity.
- System performance monitoring analyzes system performance logs in real time to look for availability problems, including active attacks (such as the 1988 Internet worm) and system and network slowdowns and crashes.

SYSTEM LOGS

A periodic review of system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours.

CONFIGURATION MANAGEMENT

From a security point of view, configuration management provides assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications. Configuration management can be used to help ensure that changes take place in an identifiable and controlled environment and that they do not unintentionally harm any of the system's properties, including its security

Changes to the system can have security implications because they may introduce or remove vulnerabilities and because significant changes may require updating the contingency plan, risk analysis, or accreditation.

Access Control

Written guidelines for access control and passwords must be documented. Guidelines must contain password requirements including the frequency of change, minimum length, character types which must be utilized.

A senior member of technical operations management must formally approve access to production systems.

LEAST PRIVILEGE

Least privilege is a policy that limits both the system’s users and processes to access only those resources and privileges necessary to perform assigned functions. When identifying users, all systems must ensure least privileges. This will be accomplished by what each user’s job is, outlining the minimum set of privileges required to perform that job, and restricting the user to only those privileges on the system/network. Users only get access to those resources necessary to do their job – no more no less. By restricting access to only those privileges necessary for performing job duties, access is denied to privileges that might be used to circumvent security.

EXTERNAL ACCESS CONTROL: FIREWALL AND DMZ

Firewalls must block or filter access between all networks. All Internet facing systems must be placed in a DMZ.

REMOTE ACCESS CONTROL

Remote access technologies consist of any technology and application that allow user access to the Zuora network when he does not have a physical LAN connection. Remote access can consist of modem or VPN through an internet service provider

Users must have unique combinations of usernames and password. Users are responsible for any usage of their usernames and passwords. Users should keep their passwords confidential and not disclose them to anyone.

Regardless of how complex the network and how the remote access services are acquired, the following security elements must be followed:

- Authentication: verify the user's login credentials and allow only those who have authorization access to the network.
- Access Restriction: to define the resources the user can access.
- Time Restriction: restricting when a user can connect and for what duration of time the connection is allowed.
- Connection Restriction: impose limit of simultaneous connections per user, consecutive failed attempts, and users of use.
- Protocol Restriction: restrict what protocols and services are available through the dial-up
- Data Encryption: Protect communication links from eavesdroppers to preserve the integrity and confidentiality of transmitted data.
- Remote access users are required to have personal firewalls and anti-virus software on their desktops to prevent another system from accessing them while connected to the remote access service.
- Remote-access technologies used by vendors and business partners should be activated only when needed by vendors and business partners, and immediately de-activated after use.

ACCESS TO CARDHOLDER DATA

Zuora requires procedures for data control to be maintained and implemented by the Technical Operations and IT departments to support the security of the CDE. Access to privileged user IDs is restricted to the least privileges necessary to perform job responsibilities.

- Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities
- Assignments of privileges are based on individual personnel's job classification and function and must be formally approved by a senior manager of the Technical

Operations department.

- Zuora requires all new access to CDE to be formally requested in the IT ticketing solution. Only after approval by a senior manager in the TechOps department and the Security team, will IT provision the access.
- Zuora shall implement an automated access control system using VPNs to restrict access and directory servers to manage user accounts.
- All production user accounts must be reviewed on a quarterly basis.

ACCESS TO ePHI DATA

Zuora requires procedures for data control to be maintained and implemented the Technical Operations and IT departments to support the security and privacy requirements of HIPAA.

- Access rights to privileged User IDs are restricted to least privileges necessary to perform job responsibilities
- Assignments of privileges are based on individual personnel’s job classification and function and must be formally approved by a senior manager of the Technical Operations department.
- Zuora requires all new access to ePHI data to be formally requested in the IT ticketing solution, only after approval by a senior manager in the Technical Operations department, will IT provision the access.
- Zuora shall implement an automated access control system using VPNs to restrict access and directory servers to manage user accounts.
- VPN access shall require two-factor authentication for granting access to systems containing ePHI data.

MOBILE DEVICES AND REMOTE ACCESS

Remote access to Zuora's computer equipment and services is only permitted for approved personnel. All remote access must be carried out over a VPN connection that utilizes multi-factor authentication for access.

Remote access to Zuora's network may only take place through security solutions approved by the IT department.

Mobile devices must be protected with full disk encryption and have Zuora’s security policies enforced by IT. Customer data must never be copied to mobile devices. All customer data must reside within production networks and is prohibited from being copied out of these networks.

THIRD PARTY ACCESS SECURITY

No external agency will be given access to any of Zuora’s networks unless that body has been formally authorized to have access. All non-Zuora agencies will be required to sign security and confidentiality agreements with Zuora. Zuora will control all external agencies access to its systems by enabling/disabling connections for each approved access requirement. Zuora will put in place adequate policies and procedures to ensure the protection of all information being sent to external systems. In doing so, it will make no assumptions as to the quality of security used by any third party but will request confirmation of levels of security maintained by those third parties.

Where levels of security are found to be inadequate, alternative ways of sending data will be used. All third parties and any outsourced operations will be liable to the same level of confidentiality as Zuora Staff.

Software Acquisition, Development, and Maintenance

The security of data and information is one of the most important elements of information system security. Thus, it is important to prevent unauthorized access and to protect the system from harm. The objectives to make sure of the availability system, integrity of the processing the data and confidentiality of the data is protected. As such, Zuora uses a variety of mechanisms, including hardware and software to process and access data in the CDE.

Application development procedures are vital to the integrity of systems. If applications are not developed properly, data may be processed in such a way that the integrity of the data is corrupted. In addition, the integrity of the application software itself should be maintained, both in term of change control and terms of attack from malicious software. In addition, if confidentiality is required for data, encryption mechanism should be built into the programming code from the beginning, and not added on as an afterthought.

SOFTWARE DEVELOPMENT LIFE CYCLE (SDLC)

Software must be developed in accordance with PCI DSS standards. This includes internal and external facing software and any web-based administrative access to applications developed by Zuora. Zuora requires software be developed using secure authentication and logging based on industry best practices. Information security is incorporated throughout all phases of the software development process. Zuora's software development security practices are founded on the Open Web Application Security Project (OWASP) top 10 project. Zuora performs routine application penetration testing to ensure the objectives of the OWASP top 10 are being achieved.

The software development life cycle, or SDLC, encompasses all the steps that an organization follows when it develops software tools or applications. Organizations that incorporate security in the SDLC benefit from products and applications that are secure by design. Those that fail to involve information security in the life cycle pay the price in the form of costly and disruptive events.

Zuora’s SDLC model must contain the following main functions:

- Conceptual definition: This is a basic description of the new product or program being developed, so that anyone reading it can understand the proposed project.
- Functional requirements and specifications: This is a list of requirements and specifications from a business function perspective.
- Technical requirements and specifications: This is a detailed description of technical requirements and specifications in technical terms.
- Design: This is where the formal detailed design of the product or program is

developed.

- Coding: The actual development of software.
- Test: This is the formal testing phase.
- Approval: Formal approval of the changes to be implemented
- Implementation: This is where the software or product is installed in production

SECURE CODING GUIDELINES

Web applications developed at Zuora must follow secure coding guidelines to prevent common coding vulnerabilities in software development process. At a minimum, software developers are trained on the following web application vulnerabilities to protect Zuora's applications.

- Injection flaws - including SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
- Buffer overflow - an anomaly where a computer program, while writing data to a buffer, overruns its buffer and overwrites adjacent memory. This can cause erratic behavior in the application and access to memory.
- Insecure cryptographic storage - This includes weak encryption algorithms, poor key management/rotation, and poor system design. For more details see OWASP's Cryptographic Storage Cheat Sheet.
- Insecure communications **-** All authentication and sensitive information must be encrypted in transit. Zuora requires all web application traffic to be encrypted in transit over untrusted networks.
- Improper error handling **-** Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Applications can also leak internal state via how long they take to process certain operations or via different responses to differing inputs, such as displaying the same error text with different error numbers. Web applications will often leak information about their internal state through detailed or debug error messages. Often, this information can be leveraged to launch or even automate more powerful attacks. For more information see OWASP's guide on Information Leakage and Improper Error Handling.
- High vulnerabilities identified by Zuora penetration testing - Zuora performs routine application vulnerability scanning using multiple tools, high vulnerabilities identified in these scans should be communicated to developers and training should be conducted to close existing vulnerabilities and prevent future releases from introducing the same vulnerabilities again.
- Cross-site scripting (XSS) **-** XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim’s browser, which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
- Improper Access Control **-** Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access

functionality without proper authorization.

- Cross-site request forgery (CSRF) - A CSRF attack forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim’s browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

DATA VALIDATION

Input data validation should include checks for out-of-range values, invalid characters in data fields, missing or incomplete data, the exceeding of upper and lower data volume limits, unauthorized or inconsistent control data, and the procedures for responding to these issues. Data balances should be validated, and data should be validated within the program.

The integrity of data and software should be checked. Message authentication should be performed.

Information systems, which have been designated "production systems" have special security requirements. A production system is a system that is regularly used to process information critical to Zuora’s business. Although a production system may be physically situated anywhere, the production system designation is assigned by the Technology Services Director of Systems and Operation.

Production systems should also have designated Stewards and Custodians for the critical information they process. The Information Security Office should perform periodic risk assessments of production systems to determine whether the controls employed are adequate. All production systems should have an access control system to restrict who can access the system as well as restrict the privileges available to these Users. A designated access control administrator (who is not a regular User on the system in question) should be assigned for all production systems.

Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is maintained in a much more rigorous way for the production system, while the other two environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff should not be permitted to have access to production systems. Likewise, all production software testing should proceed with sanitized information (where Confidential or Highly Restricted information is replaced with dummy data). All security fixes provided by software vendors should also go through the testing process, and then should be promptly installed. Application programmers should not be given access to production information. A formal and documented change control process must be used to restrict and approve changes to production systems. All program-based access paths other than the formal User access paths should be deleted or disabled before software is moved into production.

Administrative access to the production environments should not use administrative (or root) login credentials. All users should login to the jumpbox with their own unique user ID.

Administrative privileges for approved users can be gained only after the users login with their unique user IDs.

Security Checklists

A checklist should be provided against the system being audited. This list outlines the major security considerations for a system, including management, operational, and technical issues. One advantage of using a computer security plan is that it reflects the unique security environment of the system, rather than a generic list of controls. Other checklists can be developed, which include organizational security policies and practices (often referred to as baselines). Lists of "generally accepted security practices" (GASPs) can also be used. Care needs to be taken so that deviations from the list are not automatically considered wrong, since they may be appropriate for the system's particular environment or technical constraints.

Checklists can also be used to verify that changes to the system have been reviewed from a security point of view. A common audit examines the system's configuration to see if major changes (such as connecting to the Internet) have occurred that have not yet been analyzed from a security point of view.

Penetration Testing

Penetration testing can use many methods to attempt a system break-in. In addition to using active automated tools, penetration testing can be done "manually." The most useful type of penetration testing is to use methods that might really be used against the system. For hosts on the Internet, this would certainly include automated tools. For many systems, lax procedures, or a lack of internal controls on applications, are common vulnerabilities that penetration testing can target. Another method is "social engineering," which involves getting users or administrators to divulge information about systems, including their passwords.

Cryptography

Cryptography is used to protect data both inside and outside the boundaries of a computer system. Outside the computer system, cryptography is sometimes the only way to protect data. While in a computer system, data is normally protected with logical and physical access controls (perhaps supplemented by cryptography). However, when in transit across communications lines or resident on someone else's computer, data cannot be protected by the originator's logical or physical access controls. Cryptography provides a solution by protecting data even when the data is no longer in the control of the originator.

All credit card data must be encrypted while data is at rest or in transit.

Information Security Incident Management

All breaches of security, along with the use of information systems contrary to routines, should be treated as incidents. All employees are responsible for reporting breaches and suspected breaches of security. Incidents should be reported to management and Zuora's Security and Compliance team immediately.

A computer security incident can result from a computer virus, other malicious code, or a system intruder, either an insider or an outsider. It is used in this section to broadly refer to those incidents resulting from deliberate malicious technical activity. It can more generally refer to those incidents that, without technically expert response, could result in severe damage.

Although the threats that hackers and malicious code pose to systems and networks are well known, the occurrence of such harmful events remains unpredictable. Security incidents on larger networks (e.g., the Internet), such as break-ins and service disruptions, have harmed various organizations' computing capabilities. When initially confronted with such incidents, most organizations respond in an ad hoc manner. However, recurrence of similar incidents often makes it cost-beneficial to develop a standing capability for quick discovery of and response to such events. This is especially true since incidents can often "spread" when left unchecked thus increasing damage and seriously harming an organization.

Incident handling is closely related to contingency planning as well as support and operations. An incident handling capability may be viewed as a component of contingency planning because it provides the ability to react quickly and efficiently to disruptions in normal processing. Broadly speaking, contingency planning addresses events with the potential to interrupt system operations. Incident handling can be considered that portion of contingency planning that responds to malicious technical threats.

COMPUTER INCIDENT RESPONSE TEAM

The primary directive of the Computer Incident Response Team is Incident Response Management, which manages Zuora's response to events that pose risk to our computing environment.

The management consists of the following:

- Coordinating the notification and distribution of information pertaining to the incident to the appropriate parties (those with a need to know) through a predefined escalation path.
- Mitigation risk to Zuora Computing Services by minimizing the disruptions to normal business activities and the costs associated with remediating the incident (including public relations)
- Assembling teams of security technical analysts and forensic team to investigate the potential vulnerabilities and to resolve specific intrusions.
- Management of network logs, including collection, retention, review, and analysis data
- Management of the resolution of an incident, management of the remediation of a vulnerability, and post-event reporting to the appropriate parties.

COMPUTER INCIDENT RESPONSE AND PUBLIC RELATIONS

Zuora will include in the incident response procedures a predetermined action plan to address public relations issues. Being able to maintain constituent’s confidence during a period of crisis or emergency is vital to Zuora’s reputation and survivability.

Business Continuity Planning

Zuora should seek to identify the consequences of disasters, security failures, and loss of service and should develop contingency plans. Risks should be understood in the terms of their likelihood.

Regular testing, documentation, and updates are required. Updates are required if there are changes in personnel, addresses or telephone numbers, business strategy, location, legislation and changes in contractors, suppliers, and key customers.

Zuora’s Directory of Business Systems is responsible for defining a company-wide disaster recovery plan in accordance with the risks identified in Zuora’s risk assessment activities.

Disaster Recovery

Disaster recovery policies are focused on how Zuora will recover the services in the event of a disaster that disrupts operations. The Technical Operations department is responsible for defining the specific disaster recovery procedures for recovering operations to a secondary site. The disaster recovery process must be communicated to the Technical Operations team on a routine basis. A tabletop test of the disaster recovery process must be carried out at least annually.

Zuora's staff, contractors, and visitors will have the same levels of access at disaster recovery cloud region that they have at Zuora's primary cloud region in order to perform disaster recovery activities to restore system operations in the event of a disaster.

Compliance

COMPLIANCE WITH REGULATORY & LEGAL REQUIREMENTS

Zuora must comply with laws, as well as other external guidelines, such as but not limited to:

- EU-US Privacy Shield
- E.U. General Data Protection Regulation (GDPR) (EU 2016/679)
- California Consumer Privacy Act
- Payment Card Industry Data Security Standard (PCI-DSS)
- Statement on Standards for Attestation Engagements No. 18 (SSAE 18)
- Trust Services Principles Section 100 as applied in the AICPA's Guide on SOC 2
- International Organization for Standardization (ISO) Information Security Standard 27001 (ISO/IEC 27001), 27018 (ISO/IEC 27018), and 27701 (ISO/IEC 27701)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules

COMPLIANCE WITH SECURITY POLICY

All employees, contractors, and consultants must comply with the Information Security Policy and guidelines. Employees, contractors, and consultants must comply with IT regulations. Employees, contractors, and consultants should be aware that evidence from security incidents will be stored and may be handed over to law enforcement agencies following court orders.

GOVERNING DOCUMENTS FOR INFORMATION SECURITY

Purpose of Governing Documents

Governing documents for information security should contribute to a balanced level of measures with regards to the risks and requirements related to Zuora.

Documented requirements and guidelines should exist for information security based on up-to-date risk assessments. Systems and infrastructure should be covered by best practices for information security.

Document Structure

Zuora has organized a document structure describing the security architecture in three levels.

The structure for governing documents on information security is as follows:

LEVEL 1: SECURITY POLICY

Defining goals, purposes, responsibility, and overall requirements. Additionally, it gives an overview over established governing documents regarding information security and why it is important.

This document is governing information security policy documentation.

LEVEL 2: SECURITY PROCEDURES

Detail how to carry out the day-to-day activities in order to comply with Zuora’s Information Security Policy.

LEVEL 3: SECURITY STANDARDS

Contains detailed standards and configurations that address how systems are implemented to comply with security procedures (Level 2).