# Scalr Security Overview

## 1. Overview

This document provides descriptions of the policies and procedures that Scalr has in place to ensure security, data protection, and incident handling.

## 2. Terminology and Definitions

- Scalr - Refers to the company Scalr, Inc.
- Scalr.io - Refers to the software service that customers subscribe to for Terraform automation and collaboration
- Product - Refers to the products and services made available to the public including Scalr.io

## 3. Security Overview

### Product Security

Scalr has the following policies in place for product security:

Scalr follows OWASP (Open Web Application Security Project) security and development best practices.

- https://www.owasp.org/index.php/Main_Page

The OWASP Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. SAMM helps to:

- Evaluate an organization's existing software security practices
- Build a balanced software security assurance program in well-defined iterations
- Demonstrate concrete improvements to a security assurance program
- Define and measure security-related activities throughout an organization

The OWASP Software Security Assurance Process (OSSAP) main intent is to embed security in the software development lifecycle (SDLC). OSSAP reduces the possibility of requirement oversights, design flaws, implementation bugs and deployment configuration mistakes during the SDLC. This project outlines mandatory and recommended processes and practices to manage risks associated with applications.

## Software Development Life Cycle

Scalr has the following process in place for software development:

Scalr uses an SDLC process in line with the agile methodology. Scalr requires all code to be reviewed by at least one senior level engineer prior to merging into the master branch and uses a continuous integration process to release the software. Using the agile methodology, Scalr is able to detect and fix bugs and security defects faster than using a longer release cycle methodology.

## Encryption Mechanism

Scalr has the following encryption standards in place:

All data transferred to scalr.io, the Scalr SaaS platform, is encrypted using the HTTPS (TLS 1.2) protocol.

Customer passwords are hashed using the PBKDF2 algorithm with a SHA256 hash, a password stretching mechanism recommended by NIST.

Scalr.io is deployed on Google Compute Cloud. By default, Google Compute Cloud encrypts all data at rest and in transit. The data in scalr.io is also stored at rest with AES 256 encryption.

Learn more here: https://cloud.google.com/security/#dataencryption

## Single Sign-On

Scalr supports single sign-on and two-factor authentication and recommends that all customers use it. More information on this can be found here.

## Physical/Remote Security Overview

Scalr has the following physical security standards in place:

Scalr is a distributed organization with employees working in many different parts of the world. Remote offices may be used as a place to work with prior approval from HR.

All remote offices are to be secure and require keyed entry into either the office complex or office space used by Scalr personnel.

Remote access to Scalr systems is granted on an as-needed basis by the employees line manager. Access to Scalr systems is reviewed quarterly and employees must have least privileged access unless otherwise noted by their manager.

### Security Training

Scalr has the following security training in place:

Scalr employees must understand the risks in using today's technology and how to effectively defend against today's security and cyber threats, both at work and at home. The primary purpose of an effective information security training and awareness program is to establish and sustain an appropriate level of protection for data and technology resources by increasing users' awareness of their information security responsibilities.

All Scalr employees are required to complete security awareness training and training with respect to Scalr's information security policies upon hire and subsequently at least annually. Training may be delivered in person or online. The Security Training and Awareness program will also include unscheduled awareness assessments to ensure compliance with the training.

### Scalr Internal Password Policy

Scalr has the following password policy in place:

All Scalr employees have the following passwords policy enforced on their SSO accounts:

- Change every 180 days
- Require strong passwords (at least 12 chars)
- Password reuse is not allowed

## 4. Data Policy Definition

### IT Information Security Policy

Scalr has the following information security policies in place:

This policy describes how data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

The Scalr team may need to gather and use certain information about individuals and organizations. This can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

See the encryption section above for more information on how the data is protected.

## General Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Scalr will provide guidelines to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager if they are unsure about any aspect of data protection.

## Data retention and backup

Scalr has the following data retention and backup procedures in place:

Backups of the production database are automatically initiated every 3 hours and retained for 30 days. Backup data is encrypted and stored in secondary data centers.

## Privacy

Scalr has the following privacy policy in place:

Scalr respects the privacy of all of our users and does not sell or share any personal data to external parties. The full Scalr privacy policy can be found here: https://www.scalr.com/privacy-and-cookie-policy/

### Vulnerability and Patch Process

Scalr has the following vulnerability process in place:

All system components and software are to be protected from known vulnerabilities by installing applicable vendor supplied security patches. Any critical vulnerabilities must be fixed by applying critical security patches within thirty (30) days after release by the vendor. Other patches not designated as critical by the vendor shall be applied on a normal maintenance schedule as defined by normal systems maintenance and support operating procedures.

A regular schedule should be developed for security patching of all Scalr systems and servers. Patching includes updates to all operating systems, packages, databases, and third party applications.

Scalr reserves two weekly maintenance windows:

Every Tuesday and Thursday
UK : 11:00
US ET : 06:00
US PT : 03:00

Emergency patching can happen outside of those windows in the event of a vulnerability.

### Vulnerability Submission

Any vulnerability can be submitted to Scalr through our portal here.

## 5. Incident and Change Management

### Incident Response Policy

Scalr has the following incident response policy in place:

The Scalr Security Response Plan (SRP) provides the impetus for security, engineering and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, the SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. As new products or services are developed and prepared for release to consumers, the SRP ensures that when an incident occurs, swift mitigation and remediation ensues.

In keeping with GDPR requirements, Scalr will notify customers within 72 hours of a suspected breach via e-mail.

## Change Management Process

Scalr has the following change management process in place:

The Scalr change management process applies to all technology changes which may be deployed or applied to sclr.io and/or core software engineering environments.  All Scalr team members are required to abide by this policy.

The following outlines the process for submitting, reviewing, approving, deferring and closing technology change items:

Change requests are to be logged as JIRA tickets by the owner of the change. The ticket should identify the scope of the change, areas affected, back-out process, testing completed, communication plan and planned date of deployment. This to be done at a level to ensure the scope as described can be accomplished and to provide assurance that the change will have the desired result. Once a change request is submitted it will be categorized as a change item.

New change items are reviewed during team change meetings. Pending change tickets are reviewed with the group to ensure all attending understand the change and its dependencies. Items that are understood and agreed to by all are motioned for approval. Any incomplete requests will be held or deferred as decided on during the change meeting.

Authorization of a change item occurs after the change is reviewed and depends on the priority of the change ticket.

## Disaster Recovery and Business Continuity Plan

Scalr has the following disaster recover and business continuity plans in place:

Scalr infrastructure is hosted on the Google Cloud Platform. If there is a major disaster or outage affecting regions of Google Cloud where Scalr is hosted, we maintain a recovery plan that allows Scalr to run in alternate regions. Also, see the data retention and backup section above for further detail on the DR plan.

As part of the Scalr business continuity plan, Scalr accesses and mitigates risks including, but not limited to, its workforce, software and technology, and leadership. The plan is reviewed and updated regularly. Drills are conducted as needed.

## 6. Third Parties

Scalr has the following third party standards in place:

Scalr uses third party vendors to provide some services, mainly the Google Cloud Platform. More information on the GCP controls can be found here: [https://cloud.google.com/security/compliance](https://cloud.google.com/security/compliance)

Scalr maintains a standard that all third party vendors must have SOC2 compliance.

## 7. Contact Scalr

If there are any questions about any part of this document, please contact us through our portal here.