platform.sh

Security & Privacy Policy Summaries for Sales

Status	Active
Version	v1.9
Owner	Privacy Team, Security Team
Reviewed by	Joey, Erika
Date of creation	2019-02-05
Date of last review	2023-02-28
Date of last update	2023-02-28
Classification	Unclassified

Table of Contents

platform.sh

Overview

This document provides a list, with summaries, of our most requested policies as part of prospective client due diligence efforts. This document can be shared without an NDA whereas the actual policy documents can only be shared with an active NDA. Questions about this document should be addressed to your Platform.sh sales representative.

Vulnerability, Severity and Remediation Policy

Summary: The Vulnerability, Severity, and Remediation Management Policy is applicable to any asset, product, or service within Platform.sh. This policy details the taxonomy to rank vulnerabilities with the associated timeframe for remediation and/or exception.

Vulnerability Scanning and Penetration Testing Policy

Summary: The purpose of this policy is to define the requirements which the vulnerability scanning and penetration testing processes need to fulfill (both for compliance and best-practice reasons). If these activities are not carried out by Platform.sh in their entirety but instead leverage the help of third party entities, then it is also described in this policy (division of responsibilities). Its scope includes both the Grid and Dedicated infrastructures, as well as Accounts and the Platform.sh API.

IT Security Policies

Summary: Instead of a single and large IT Security Policy, Platform.sh has created individual, easy to understand, IT Security Policies. The aggregate of these forms Platform.sh's IT Security Policy. This approach allows us to be myopic on important topics while still retaining usefulness and readability. Each policy is reviewed and approved by Platform.sh's management team.

It is important to note that this document lists company-wide approved policies. Platform.sh has additional policies, not listed in this document, which have not gone through a review cycle but are still valid for their target audience.

Password Reset Policy

Summary: As per the password policy, access to an account or service must each have its own unique set of credentials. It is generally accepted that this can lead to instances where credentials can be lost or forgotten, thus preventing access to systems necessary to perform critical job functions.

The purpose of this policy is to establish a standard for recovering access to an account or service where the access credentials were forgotten/lost.

The scope of this policy includes all personnel who:

- have or are responsible for an account (or any form of access that supports or requires a password) on any system that is owned by Platform.sh, or;
- have access to Platform.sh's internal services, customer data, or customer sites, or;
- store any non-public Platform.sh information.

The scope of this policy includes passwords, and multi-factor authentication (MFA), created for use on internal systems and third-party sites.

Password Policy

Summary: The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change. This policy complies with PCI standards. The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any company facility, has access to the company network or services, or stores any non-public Platform.sh information. The scope of this policy includes passwords created for use on third party sites such as Amazon Web Services and Microsoft Azure.

Vendor Management Policy

Summary: The purpose of this policy is to establish that Platform.sh will perform a mandatory review of all suppliers before entering into an agreement with the supplier. The objective of this review is to make sure that the supplier is legally aligned with Platform requirements and economically sustainable. A new supplier should bring value that no other existing provider provides. This policy also ensures that all suppliers undergo security and privacy reviews as required by applicable laws and standards.

GDPR Policy

Summary: The purpose of this policy is to establish that Platform.sh will abide by, and implement any changes required by, the GDPR.

Data Retention Policy

Summary: The purpose of this policy is to establish data retention periods that align with GDPR, PCI, and other best practices. This policy applies company-wide to all production, staging, and development systems as well as any suppliers holding personally identifiable information (PII).

Data Breach Policy

Summary: The purpose of this policy is to mandate the need for, and execution of, a data breach procedure that complies with the EU General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), as well as IT best practices.

The scope of this policy covers two main areas:

1. Personal data breaches relating to accounts.platform.sh or any of our vendors.
2. Project data breaches in which Platform.sh was the at-fault party.

This policy does not apply to any incidents in which there was no breach of data. With this in mind, if there is a reasonable assumption of a data breach, but no proof that a breach has happened, this policy may be enforced and actions taken as if a breach had occurred. The Data Protection Officer would be responsible for making the determination as to enforcement. A decision may be made to only enact a partial response if there is no proof of a breach and/or the data in question is deemed inconsequential.

Data Access Policy

Summary: Unauthorized access, breach of confidentiality, loss of integrity, disruption of availability, and other risks threaten Platform.sh resources. This policy protects our resources by establishing rules that reduce exposure of those resources to threats.

Firewall Policy

Summary: The purpose of this policy is to describe the main requirements our network needs to fulfill to be considered secure. The requirements are set specifically towards firewall and router configurations. The scope of this policy includes both the Grid and Dedicated infrastructures.

Anti-malware and Software Update Policy

Summary: The number of computer security incidents related to malware and viruses, and the resulting cost of business disruption and service restoration, continue to escalate. Implementing antimalware and antivirus systems are best practice actions that have been codified in compliance standards such as PCI and SOC 2, as well as seen in several contractual requests. This policy applies company-wide, to all locations, employees, contractors, and interns.

Acceptable Use Policy

Summary: The purpose of this policy is to outline the acceptable use of computer equipment and resources at Platform.sh by Platform.sh employees and contractors. These rules are in place to protect both Platform.sh and our employees. Inappropriate use exposes us to risks including virus attacks, compromise of network systems and services, and legal issues. This policy applies to the use of information, electronic and computing devices, network resources, cloud resources, and online services used to conduct business or interact with internal networks and business systems, whether owned or leased by Platform.sh, our employees, or a third party. This policy applies to all employees, contractors, and interns. This policy applies to all equipment that is owned or leased by Platform.sh, employees, contractors, and interns.

All employees are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with policies and standards, and local laws and regulations applying in the jurisdiction in which they are performing business-related tasks.

Risk Management Policy

Summary: Risk Management is the function used to determine both the likelihood and impact on availability, confidentiality, and integrity of data that is processed, transmitted, or stored in a given environment. The results address corporate technology risks and associated remediation activities. The objectives of this process are:

- Identify relevant technology risks affecting our assets
- Determine a risk treatment plan for identified risks
- Track improvement and risk mitigation tasks

Technology risk management activities are performed for Platform.sh-owned or Platform.sh-managed systems. Customer-owned or customer-managed systems are excluded and are the responsibility of the customer.

Cryptographic Policy

Summary: This policy and supporting procedures are designed to 1) ensure proper and effective use of cryptographic controls across the company to protect the confidentiality, authenticity, and integrity of information, 2) provide general principles under which business information should be protected, and 3) ensure proper use, protection, and management of cryptographic keys throughout their whole lifecycle. Compliance with the stated policy and supporting procedures helps to ensure the safety and security of Platform.sh system resources.

Anti-Bribery Policy

Summary: Platform.sh is committed to the practice of responsible corporate behavior and to complying with all laws, regulations, and other requirements that govern the conduct of our operations. Platform.sh is fully committed to instilling a strong anti-corruption culture and is fully committed to compliance with all anti-bribery and anti-corruption legislation including, but not limited to, the UK Bribery Act 2010 and LOI n°2016-1691 and ensures that no bribes or other corrupt payments, inducements or similar are made, offered, sought or obtained by us or anyone working on our behalf. This policy defines acts considered to be bribery (including payments, donations, hospitality, and gifts), the consequences of failure to adhere to the policy, responsibilities, as well as due diligence.

Business Continuity and Disaster Recovery Plan

Summary: This document establishes the plan used to recover the Platform.sh PaaS quickly and effectively following a service disruption that falls beyond the scope of our Incident Management process.

The PaaS is the single most important component of our company. Other traditional business processes such as finance and payroll have been designed to be independent of the PaaS and use SaaS vendors with appropriate recovery targets. Thus, those business processes are not covered in this document.

Additionally, we are an online-only company. While we do maintain some physical offices to allow for co-working and gatherings, all activities of consequence happen online and can be performed anywhere there is an internet connection. Aside from employee laptops, we have no physical assets. Instead, we use online, cloud hosting, infrastructure as a service (IaaS) providers such as Amazon Web Services (AWS).

This document is limited to the PaaS infrastructure components located in Amazon Web Services (AWS), Microsoft Azure (Azure), Google Cloud Platform (GCP), Orange Cloud (Orange), and OVHcloud data centers. The procedures are designed to recover the primary functions of the Platform.sh PaaS within 24 hours, with follow-on, clean up work extending beyond that depending upon the nature of the incident.

Data Destruction Policy

Summary: All employee and customer data should be disposed of when it is no longer necessary for business use, provided that the disposal does not conflict with our data retention policies, our customers' data retention policies, a court order, or any of our regulatory obligations.

Incident Management Policy

Summary: An incident is an unplanned interruption of service to more than one environment, caused by a failure or error in the infrastructure or products provided by Platform.sh. An incident may affect all services or a single component.

For the purposes of Incident Management at Platform.sh, there are two levels of Incidents.

- Those affecting Production environments (live sites)
- Those affecting non-production environments (staging, development sites, project UIs)

All incidents require an incident response according to the documented Incident Management procedures, however, the process is slightly different for each of the two levels.

Security Incident Management Policy

Summary: This policy provides some general guidelines and procedures for dealing with computer security incidents. This material is meant to outline what Platform.sh security personnel do when a security incident is declared and escalated.

The steps involved in handling a security incident are categorized into five stages: protection of the system; identification of the problem; containment of the problem; eradication of the problem; recovering from the incident and the follow-up analysis. This Security Incident Management Policy is one component of a comprehensive Information Security and Compliance Program at Platform.sh and must be followed by a member of the security team or an engineer expressly designated by the team, such as on-call operations staff. A computer security incident can occur at any time of the day or night. As a result, the Security Incident Management team must be on-call at all times.

PCI Policy

Summary: The Payment Card Industry Data Security Standard (PCI-DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

While we do not handle credit cards, many of our customers do. Being PCI-DSS compliant provides a level of trust to our clients and eases the yearly PCI-DSS recertification workload that we do for our clients as well as our client's workload.

Mobile Device Policy

Summary: Mobile devices, such as smartphones and tablet computers, are important tools for the organization, and Platform.sh supports their use to achieve business goals. However, mobile devices also represent a significant risk to data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the organization's data. This can subsequently lead to data leakage and system infection. Platform.sh has a requirement to protect its information assets in order to safeguard its customers, intellectual property, and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices and applications.

Operations and Software Engineering Change Management

Summary: This document contains the tasks to be completed for carrying out modifications to Platform.sh infrastructure in accordance with PCI DSS Requirement 6.4. When modifying the infrastructure it is critical that certain procedures are followed to protect the integrity of the Platform.sh product. Software Engineering and Change Management includes tasks that must be completed by Platform.sh personnel, including, employees, product owners, and management.

Change Management applies to Grid, Dedicated, Accounts, and Auth as well as to internal and external stakeholders, employees, contractors, interns, or any variations thereof that require access to Platform.sh systems and/or facilities.