Security & Privacy Policy Summaries

platform.sh

platform.sh

Table of Contents

Overview	**3**
Vulnerability, Severity and Remediation Policy	**3**
Vulnerability Scanning and Penetration Testing Policy	**3**
IT Security Policies	**3**
Password Policy	**4**
Vendor Management Policy	**4**
GDPR Policy	**5**
Data Retention Policy	**5**
Data Breach Policy	**5**
Data Access Policy	**6**
Firewall Policy	**6**
Antivirus and Software Update Policy	**6**
Acceptable Use Policy	**6**
Risk Management Policy	**7**
Cryptographic Policy	**7**
Anti-Bribery Policy	**7**
Business Continuity and Disaster Recovery Plan	**8**
Data Destruction Policy	**8**
Incident Management Policy	**9**
Security Incident Management Policy	**9**
PCI Policy	**9**
Mobile Device Policy	**10**

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 Policy applies to any asset, product, or service within Platform.sh, including but not limited to Platform.sh services, Blackfire, and Upsun SaaS environments. This policy details the taxonomy and process to rank vulnerabilities with the accompanying timeframe for remediation and/or exception granting.

Vulnerability Scanning and Penetration Testing Policy

Summary: The purpose of this policy is to facilitate procedures related to vulnerability scanning and penetration testing. This is achieved by describing the main requirements these procedures need to fulfill. This policy applies to both the Platform Grid (which includes all services delivered through Upsun SaaS environment) and Platform Dedicated product, along with 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 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, but not limited to, Amazon Web Services, Microsoft Azure, and Google Cloud Platform.

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.sh 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.

Privacy and Data Protection Policy

Summary: The purpose of this policy is to establish that Platform.sh will abide by the GDPR. Explain how Platform.sh will protect and safeguard Personal Data, and explain how we monitor and update compliance.

Data Retention Policy

Summary: The purpose of this Data Retention Policy is to establish a clear framework for managing and storing data within Platform.sh. In an era where data is crucial for operational success and compliance, it is imperative to ensure that all data is handled responsibly, retained only as long as necessary, and disposed of appropriately. This policy supports our commitment to data protection, regulatory compliance, and operational efficiency.

Data Breach Policy

Summary: This policy outlines the procedures and responsibilities for identifying, responding to, managing, and reporting personal data breaches in compliance with applicable data protection laws and regulations. This policy applies to all employees, contractors, and third-party service providers who process personal data on behalf of the organization.

Data Access & Classification 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 the exposure of those resources to threats.

Data access control is critical for the company's operation. Management is committed to appropriately classifying and maintaining access to data.

Firewall Policy

Summary: The purpose of this policy is to facilitate firewall-related procedures. This is achieved by describing the main requirements that a network needs to fulfill to be secure and compliant. This policy applies to Grid (which includes all services delivered through Upsun SaaS environment) and Dedicated.

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: This Acceptable Use Policy outlines the permitted and responsible use of Platform.sh computer systems, networks, information assets, and related resources by all Platform.sh personnel. Its purpose is to ensure that individuals understand their responsibilities in using company-provided technology and data in a secure, ethical, and lawful manner.

The policy sets expectations around appropriate behavior when accessing, storing, transmitting, or processing company and customer data, and helps reduce the risk of security incidents, data misuse, and operational disruption.

By adhering to this policy, Platform.sh personnel contribute to maintaining a secure and trustworthy environment that protects both internal systems and the information entrusted to us by our customers and partners.

Risk Management Policy

Summary: This policy describes why Platform.sh implements Risk Management, how risks are classified and rated, how identified risks are treated, and how often risk assessments are conducted. This policy applies company-wide, to all Platform.sh locations and all employees (full time, contractors and interns).

Technology risk management activities are performed for Platform.sh owned or Platform.sh managed systems.

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 to recover the Platform.sh PaaS and the Blackfire APM 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.

For the Platform.sh PaaS, this document is limited to the infrastructure components located in AWS, Azure, GCP, Orange, and OVHcloud data centers.

For the Blackfire APM, this document is limited to the infrastructure components located in AWS.

We are an online-only company and we have no physical assets. Instead, we use online, cloud hosting, and 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 employees, clients, vendors, and contractors have a personal responsibility to keep information secure and confidential. This policy aims to prevent unauthorized disclosure of information assets by the controlled disposal and destruction of media-storing confidential data.

Security Incident Policy

Summary: This policy establishes the principles governing the identification, classification, and notification of security incidents affecting Platform.sh services and projects. It defines the obligations of Platform.sh regarding incident response communication in accordance with applicable laws and industry best practices.

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 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.

Risk governance policy

Summary: This Policy outlines the principles, structure, and processes of how Platform.sh identifies, assesses, manages, and monitors risk. Risk governance is a strategic business function that helps ensure that risk management activities align with the Platform.sh opportunity and loss capacity and leadership's tolerance of it and the risk management strategy is aligned with the overall business strategy.

AI Policy

Summary: This Policy aims to enable AI-powered technology to protect Personally Identifiable Information (PII) and our Intellectual Property (IP) while maintaining compliance with applicable legal, contractual, and industry-standard requirements.

Child safety policy

Summary: Platform.sh reports apparent instances of child exploitation (file locations only, and never actual material) and missing children detected on our services to regional authorities. For instructions on how to navigate the technical aspects of handling suspected child exploitation, please follow our procedure here.

Environment Segregation Policy

Summary: Having Development and Testing environments separated from Production is a security best practice that maintains our security posture by allowing us to find and fix bugs before moving into Production as well as helping us to reduce the risks of inadvertent or unauthorized modifications that could compromise the system's integrity or availability. Furthermore, it keeps us compliant with various security standards and frameworks.

Governmental Authority Data Request Policy

Summary: This policy outlines the procedures that Platform.sh will follow when responding to requests for data or information from governmental authorities, including law enforcement agencies, regulatory bodies, or courts. The policy ensures that any such requests are handled in compliance with applicable laws, the protection of user privacy, and the company's ethical standards

Abuse report policy

Summary: The purpose of this policy is to set out Platform.sh's procedure for handling Abuse Reports regarding illegal content hosted on Platform.sh and implement a policy for notifying affected customers of Abuse Reports against them.

HIPAA policy

Summary: This policy establishes guidelines to ensure compliance with HIPAA for the protection of Protected Health Information. This policy applies to all employees, contractors, business associates, and third parties who handle PHI on behalf of the organization.