Security Overview

Product, Process, Data Centre & Network Security

This document details our security practices in relation to our product, processes, data centre and network security.

Overview

Pactly is a contract review & management platform that helps legal teams with all aspects of their contracting process. Our clients use Pactly to automate routine tasks, reduce the time spent preparing and negotiating contracts, and leverage their historical contract data to drive better outcomes for their businesses in contract negotiations.

Pactly runs on a software-as-a-service (SaaS) model and offers its services through a fully managed cloud infrastructure hosted on Amazon Web Services (Singapore). Pactly is ISO 27001 certified.

Pactly Data Center & Network Security

Physical Security	
Facilities	Pactly's physical infrastructure is hosted and managed within Amazon's secure data centres and utilises Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance with industry standards. Amazon's data centre operations have been accredited under ● ISO 27001 ● SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II) ● PCI Level 1 ● FISMA Moderate ● Sarbanes-Oxley
On-site Security	Pactly utilises ISO 27001, and FISMA certified data centres managed by Amazon. AWS data centres are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms and other natural boundary protection. Physical access is strictly controlled at the perimeter and building ingress points by professional security staff utilising video surveillance, state-of-the-art intrusion detection systems, and other electronic means. Authorised staff must pass two-factor authentication no fewer than three times to access data centre floors. All visitors and contractors must present identification and are signed in and continually escorted by authorised staff.
Location	Pactly service providers' data centres are located in Singapore.

Network Security	
Protection	All firewall infrastructure and management is provided by our service provider: Amazon AWS. Firewalls are utilised to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business needs. Each system is assigned to a firewall security group based on the system’s function. Security groups restrict access to the ports and protocols required for a system’s specific function to mitigate risk. Host-Based firewalls also provide the ability to limit inbound and outbound connections further as needed. Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor, which will not deliver traffic to an interface it is not addressed to. Our service provider utilises application isolation, operating system restrictions, and encrypted connections to ensure risk is mitigated at all levels. Port scanning is prohibited, and our infrastructure provider investigates every reported instance. When port scans are detected, they are stopped, and access is blocked.
Web Application Firewall	Pactly leverages Cloudflare’s WAF that automatically blacklists and blocks malicious traffic.
Penetration Testing and Vulnerability Assessments	Third-party security testing of our service provider is performed by independent and reputable security consulting firms. Findings from each assessment are reviewed with the assessors, risk ranked, assigned to the responsible team for remediation and then reviewed again.
Security Incident Event and Response	In the event of a security incident, our engineers are called in to gather extensive logs from critical host systems and analyse them to respond to the incident in the most appropriate way possible. Gathering and analysing log information is critical for troubleshooting and investigating issues. Our service provider allows us to analyse four main log types: system, application, API logs and audit logs from user accounts. Further, in the event of a high criticality incident, Pactly will notify affected customers (if identifiable) or all customers if Pactly is unable to identify the affected customers.
DDoS Mitigation	Our service provider’s infrastructure provides DDoS mitigation techniques, including TCP Syn cookies and connection rate limiting, in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to respond quickly to events and enable

	advanced DDoS mitigation controls when needed. In addition, traffic to our services is routed through Cloudflare, which provides another layer of DDoS mitigation.
Logical Access	Access to the Pactly Production Network is restricted by an explicit need-to-know basis. It utilises the principle of least privilege, is frequently audited and is closely controlled by our Engineering Team.

Encryption

Encryption in Transit	Communications between customers, vendors, and Pactly servers are encrypted via industry best practices (HTTPS).
Encryption at Rest	Pactly encrypts sensitive customer data at rest.

Availability & Continuity

Uptime	Pactly availability has been 100% for the previous quarter and is continuously monitored. The availability reports are available at https://status.pactly.com/
Redundancy	Pactly leverages a cloud-native architecture, including clustering, to eliminate a single point of failure.
Disaster Recovery	Pactly's platform is designed to monitor its systems and automatically recover from most failures. We have stringent backup policies and audit our backups regularly. Comprehensive disaster recovery exercises are run every year.

Application Security

Secure Development (SDLC)

Framework Security Controls	We utilise secure development best practices to limit exposure to OWASP's Top 10 security flaws. These include inherent controls that reduce our exposure to Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and SQL Injection (SQLi), among others.
QA	We employ automated testing and continuously scan our code base and images for security issues. Application engineers on staff identify, test, and triage security vulnerabilities in code.

Separate Environments	Testing and staging environments are separated from the production environment. No actual customer data or vendor data is used in the development, staging, or test environments.
Secure Credential Storage	Pactly follows secure credential storage best practices by never storing passwords but instead storing a one-way hash of the salted password.
API Security & Authentication	Pactly API is TLS only, and you must be a verified user to make API requests. APIs are rate limited to prevent brute force attacks.

Application Vulnerabilities

Static Code Analysis	Our source code repositories and application images are continuously scanned for security issues via analysis tools integrated into our continuous deployment workflow.
Dependency Analysis	Our application dependencies are continuously scanned for CVE information and remediated when fixes are released.

Additional Product Security Features

Access Privileges & Roles	Access to view and change your Pactly account configuration is governed by access rights and can be configured to define access privileges. Pactly has various default permission levels available for use (administrator, manager, user, etc.).
Account audit logs	Pactly accounts include an audit log of the activity in the account. This data is available via the UI but can also be accessed from the API for automated collection and centralisation of event data.
Authentication Options	In addition to standard password-based authentication, Pactly supports 2FA (two-factor authentication).
Transmission Security	All communications with Pactly servers are encrypted using industry-standard HTTPS. This ensures that all traffic between you and Pactly is secure during transit

Additional Security Measures

Security Awareness, Employee Vetting	
Security Awareness Policies	Pactly has a comprehensive set of security policies covering a range of topics. These policies are shared with and made available to all employees and contractors with access to Pactly information assets.
Security Awareness Training	All new employees attend Security Awareness Training, and the Engineering Team provides security awareness updates via internal communication tools.
Employee Vetting	Pactly performs background checks on all new employees following local laws. All new hires are screened through the hiring process and must sign a contract with clear confidentiality provisions.