Poka Security Policy

Effective Date: September 2, 2021

1. Applicability

The purpose of Poka's Security Policy is to define the activities associated with the provision of security activities that protect information systems, networks, data, databases and other information assets in relation to the Software Services. All terms not defined herein shall have the meaning set forth in Poka's Customer terms of service #to add LINK

2. Human Resources

2.1 **Background Checks.** All potential employment candidates are required to successfully complete a standard background check as part of Poka's hiring process.

2.2 **Policies.** All of Poka employees and contract personnel are required to sign Poka's applicable internal policies for the management of Client Data including data security, confidentiality and integrity.

2.3 **Employment agreements.** Poka's employment agreements include standard confidentiality and non-disclosure obligations for employees.

2.4 **Training.** Poka provides mandatory and annual information security training for all employees updated from time to time to cover new security threats, technical developments or applicable law requirements.

3. Software Services Delivery Model

3.1 The Software Services are provided based with maintenance, updates and bug fixes being released or deployed on a continuous basis. The automated nature of the Software Services and infrastructure delivery, combined with frequent releases, requires that the security be embedded into Poka's software development life cycle (SDLC) including but not limited the following security, privacy and quality assurance practices: requirements identification, requirements review, design reviews, development controls (e.g., static analysis, code reviews), automated and manual testing, automated vulnerability scans, change management and deployment controls.

4. Data Encryption

4.1 Poka support the latest recommended secure cipher suites and protocols to encrypt data in transit. Client data is encrypted in transit using Transport Layer Security (TLS) 1.2 and encrypted at rest using 256-bit AES, one of the strongest block ciphers available.

4.2 Poka monitors the changing cryptographic landscape closely to update the Software Services to respond to new cryptographic weaknesses as they are discovered and implement best practices as they evolve and taking into account compatibility.

4.3 Poka enforces the usage of full disk encryption for all company devices.

5. Tenant Isolation

5.1 To ensure data isolation, each Client is given a dedicated instance, segregated database and data stores for the Software Services application.

6. Subscribed Users Identity Models and Authentication

6.1 Client can integrate the Software Services with corporate credential directories using Security Assertion Markup Language (SAML v2.0) to retain full control of authentication process. Client can also automatically provision and deprovision Subscribed Users with Poka's system for Cross-domain Identity Management (SCIM) compatible API - an open standard used by identity providers and Single Sign-On (SSO) services to manage user accounts across of software services providers. Client can also manage Subscribed User accounts directly in the Software Services application. Credentials are never stored in human readable format. Poka uses a secure one-way hash algorithm with a salt.

6.2 Access to Client instance is governed by roles and access rights configured by Client's designated Poka Administrators.

7. Logical Firewall

7.1 Client may choose to restrict access to a specific IP range so that their instance is only accessible in designated physical locations and through their VPN. Poka also support a per Subscribed User access policy that enables them to connect outside Client designated physical locations. Client can also restrict from which countries they are allowed to access the instance using Poka's IP Geolocation access control feature.

8. Backups and Disaster Recovery

8.1 Client Data is stored redundantly at multiple locations in Poka's hosting provider's data centers to ensure availability. Client data is backed up every hour and replicated in near-real time at the designated secondary Amazon AWS Region. Backups are performed without impacting the availability of Client Data. Poka's operations and IT infrastructure can therefore easily be recovered and restored whenever required and Poka regularly test its disaster-recovery measures to ensure adequate resolution from a major disaster.

9. Network Protection and Logging

9.1 Poka's information technology infrastructure uses a variety of controls to ensure the protection and isolation of the environments, servers, containers, subnets such as logical firewall, web application firewall, application Load Balancers, etc. to ensures that only authorized traffic from the internet or corporate network between servers are allowed. Logs are generated and analyzed for security events via automated monitoring software managed by Poka's security team.

10. Vulnerability Management

10.1 Poka performs automated vulnerability scans on our production environment and remediate any findings that present a risk to Poka's IT infrastructure. Additionally, penetration testing against Poka's production environment is performed on an annual basis by a qualified third party.

11. Hosting Infrastructure

11.1 Poka uses Amazon Web Services for the hosting of all Client instances. For more information about their certification and compliance program, please visit the AWS Security website and the AWS Compliance website.

12. Compliance

Poka maintains the following security and compliance certifications for the Software Services:

12.1 **SOC 2 Type II.** Poka is compliant with the Service Organization Controls (SOC) 2 Type 2 from AICPA, an industry standard security attestations for Software as a Service providers. The SOC 2 Type 2 report confirms that Poka's information security program and control environment are compliant with the trust services criteria developed and maintained by the AICPA. The report covers the controls Poka has implemented both from an organizational and technical perspective, and includes access management, encryption, code changes and deployment, monitoring, vulnerability management, incident management, risk management, human resources management, vendor management, and more. Poka's SOC 2 Type 2 report is available upon request.

12.2 **Poka's response to the Cloud Security Alliance Questionnaire.** The Cloud Security Alliance (CSA) is a nonprofit organization led by a broad coalition of industry practitioners, corporations, and other important stakeholders. It is dedicated to defining best practices to help ensure a more secure cloud computing environment, and to helping potential cloud customers make informed decisions when selecting a cloud vendor. The Security, Trust, and Assurance Registry (CSA STAR) and the CSA Consensus Assessments Initiative Questionnaire (CAIQ) v3.0.1 provides a comprehensive set of questions that organizations can use to evaluate the service providers' security, privacy, and compliance processes. Poka's security team has compiled responses to all 294 questions in the questionnaire. This document can be accessed and downloaded here and is a valuable resource to understand how Poka meets and exceeds the requirements set forth by CSA.

12.3 **Canadian Controlled Goods Program.** The Controlled Goods Program (CGP) was initiated in April 2001 to further strengthen and coordinate defense trade controls with the U.S. The Controlled Goods Program. It is a compliance program that regulates access to controlled goods and technologies, including ITAR-controlled articles in Canada. Since 2017, Poka is registered (CGP #20710) and complies with the requirements of the Canadian Controlled Goods Regulation and the Defence Production Act which requires conducting security assessments of personnel, preparing for inspections, developing security plans and reporting security breaches.

12.4 **Data Processing.** Poka is compliant with European Union data protection laws around international data transfer mechanisms. To this extent Poka's Data Processing Agreement (DPA) covers the transfer of Client Data under Regulation (EU) 2016/679 of the European Parliament (GDPR).

12.5 **Data breach and incident management.** In the event of a security breach, Poka will promptly notify Client of any unauthorized access to Client Data. Poka has an incident management process to manage the entire lifecycle of a security breach.