Information Security Policy

Last Updated: 01 January 2025

This Security Policy ("**Policy**") details Akeyless' security program, and is updated from time to time to ensure accuracy of this Policy, provided that the levels of security will not be reduced in a material way. This Policy is an overview of the means taken by Akeyless to ensure compliance with various security requirements, including NIST, NIS2, DORA and other applicable regulations.

This Policy may be referred from the agreement signed between Akeyless Security Ltd. or its subsidiaries and affiliated companies (together, herein after "**Akeyless**") and the Customer using the Akeyless Services ("**Agreement**") and shall be a binding governing policy to ensure Akeyless' security obligations are met. This Security Policy is an integral part of the agreement governing the use of the Akeyless Services.

Definitions used herein, however not defined, shall have the meaning assigned to it in the applicable Agreement, or can be viewed in the Akeyless EULA: https://www.akeyless.io/end-user-license-agreement/.

This Policy provides an overview of the security, technical and organizational measures taken by Akeyless.

1. **Certifications and Compliance Programs**
   - 1.1. Akeyless' operations, policies and procedures are audited regularly to ensure that it meets all standards expected of it as a cloud system provider. Compliance certifications and attestations are assessed by a third-party, independent auditor and result in a certification, audit report, or attestation of compliance.
   - 1.2. Akeyless is audited and verified under the ISO 27001 and ISO 27701 certifications and the System and Organization Controls (SOC), PCI DDS. If you wish to be provided with such certifications and reports, please contact us at: privacy@akeyless.io.

2. **Management Involvement and Overall Security Management**
   - 2.1. Akeyless data security practices are anchored in a robust control environment, defined by a strong awareness and attitude towards internal controls from its management under the supervision of the board. Authority and responsibility are clearly defined and communicated through organizational structures and policies.
   - 2.2. Management, including the DPO and CISO, routinely assesses risks and compliance, emphasizing security and confidentiality. Human resources policies strengthen this framework, focusing on hiring competent personnel, providing necessary training, and ensuring compliance with security policies.

3. **HR Security Measures**
   - 3.1. Subject to applicable laws and availability, background checks and screening processes are conducted on employees and contractors prior to providing them access to any data or information.

3.2. All employees and contractors sign industry standard confidentiality clauses and data protection clauses (or data processing agreement, as applicable), prior to accessing any data or information. These clauses and agreement, include, among others, the employees/contractors commitment to not disclose proprietary or confidential information, including Customer information, to unauthorized parties or to use any such information for any other purpose other than performing Akeyless' obligations under the Agreement.

3.3. Each employee is subject to Akeyless' security policies and specifically the acceptable use policy ("**AUP**") which restricts the use and access to Akeyless' systems and device, and Akeyless' Code of Conduct.

3.4. Akeyless places a strong emphasis on security awareness and training for all employees, recognizing the importance of understanding their information security responsibilities. This is achieved through the communication of security policies and guidelines, underpinned by the Akeyless security awareness program. A mandatory annual security awareness training program is in place for all employees. This training covers critical areas such as common security risks and threats, compliance with regulations, understanding of the AUP, information security practices, data protection and customer privacy, laptop security, and awareness of social engineering tactics including fraud and phishing.

3.5. Workstations are secured using industry standard technology and practices, including, at minimum, firewalls, disk encryption, anti-virus software, password protected lock screens, any remote access to Akeyless resources and data assets is regulated behind MFA mechanisms, in order to enforce and ensure stringent security measures, clear desk and clear screen policy, and revoke access after failed attempts.

3.6. In the event of a breach of an employee's obligation or non-compliance with the aforesaid policies, Akeyless will include repercussions to ensure compliance with the policies and sanctions will be taken.

4. **Change management**

4.1. Akeyless will maintain a change management program which outlines the procedures that address the types of changes, required documentation for the changes, peer review, approvals for changes, and emergency changes.

4.2. Akeyless will use and secure only authorized version control systems.

4.3. Changes must be reviewed and approved by authorized personnel, who must be different from the person proposing the change. All changes need to be documented.

4.4. The change has to be tested and mandatory tests must pass before being merged or deployed to production.

4.5. Production and non-production environments will be kept separate. Akeyless will use a test environment separate from the production environment for testing changes.

4.6. Akeyless will publish release notices for each new major and minor release of the products.

5. Access Control, User, and Permissions Management

5.1. Akeyless implements stringent access control and user permissions management to ensure the security of its information assets. Access is strictly limited to what is necessary for an employee's or contractor's role, governed by group-based permissions aligned with job descriptions and responsibilities.

5.2. Access permissions are regularly reviewed and approved.

5.3. Akeyless enforces robust password standards, including requirements for character complexity and password history. Specifically, under systems and applications that access Customer Data Akeyless will enforce high standard password requirements.

5.4. Additional security measures include controlled system resource access, especially for higher privilege accounts, and enforced security settings on company laptops such as encryption, and remote wipe capabilities.

5.5. As detailed above, in Section 3, Akeyless shall implement and enforce multi-factor authentication for applications and systems where technically feasible and legally required (i.e., due to sensitivity of the data of importance of the feature).

6. Production System Access

6.1. Akeyless maintains rigorous access controls within its production environment to safeguard system integrity and data security. Access to the production environment is heavily restricted, with two-factor authentication, ensuring that only authorized personnel gain entry.

6.2. For backup access, alterations and deletions are strictly controlled, accessible only to authorized users and again protected by two-factor authentication. The same level of security applies to source control and sensitive database access, ensuring robust protection against unauthorized changes or data breaches.

7. Physical Access and Visitors

7.1. Physical access to the offices is restricted to authorized personnel using a designated key-code or key. The premises are further protected through an alarm system and a 24/7 manned receptionist or guard at the entrance to the building.

7.2. Visitors are required to be always accompanied by an Akeyless employee during their stay. Employees encountering an unfamiliar or suspicious person wandering around the office are expected to ask them politely about the nature of their business and if necessary, accompany them to their host. Visitors are not allowed to access or connect to Akeyless company's network or equipment.

7.3. Akeyless data center security is reinforced through its reliance on well-known major cloud services providers' global infrastructure, which encompasses facilities, networks, hardware, and operational software. Currently Akeyless uses AWS, GCP and Azure. This infrastructure adheres to stringent security best practices and complies with various security standards and regulations, including ISO 27001, 27017 and 27018, and SOC2, among other certifications and reports.

7.4. The data centers' facilities provide redundant power, redundant backup generators, and redundant cooling systems. Physical access to data center floor space housing Akeyless cloud-based Services is secured according to industry-standard best practices, and include security cameras, proximity cards,

biometric scanners, mantraps, and complete access logging, or equivalent measures

7.5. Please see sub-contractor list and table below, for more information on the security measures addressed.

8. Network and Infrastructure Security

8.1. Akeyless will maintain baseline configurations for infrastructure deployed and used within the production environment. Akeyless will maintain mechanisms in place to ensure that baseline configurations are applied and maintained. All sensitive data transmitted and processed within public networks will be encrypted in transit and at rest.

8.2. Akeyless will not use Customer Data in non-production environments or for testing on local developer machines.

8.3. Akeyless employs a managed configuration system for server and patch management, maintaining hardened security settings across devices. This is complemented by endpoint protection on employee devices through the utilization of an EDR system, and restricted software installation, ensuring a secure and controlled application environment (i.e., generally, no admin authorizations at host-level).

8.4. Akeyless employs robust data encryption strategies to protect both data in transit and data at rest, enhancing its overall data security posture. For data in transit, the company ensures secure communication between its customers and company assets through the use of HTTPS with TLS 1.2 authenticated certificates as a minimum. All restricted information assets, such as databases and backups containing customer data, are encrypted at least at the disk level.

8.5. Moreover, Customer Data stored at rest is automatically encrypted using multiple encryption mechanisms to protect Customer's secrets, in a layered encryption approach that ensures a high level of security for stored data, mitigating risks and enhancing Customer trust. For more information, please see: https://www.akeyless.io/dfc-technology/

9. Risk Assessment and Vulnerability Management

9.1. Having a pre-defined clear and detailed risk assessment strategy is integral to Akeyless data security framework, focusing on identifying, analyzing, and mitigating risks that could impact its objectives and its Services. This involves a thorough evaluation of information assets, threats, and vulnerabilities, both internal and external.

9.2. Akeyless employs a formal risk management program, continuously addressing information security risks through a variety of treatment options like acceptance, avoidance, mitigation, and transfer. Key decisions on risk treatment are documented and approved annually by management (as part of the ISO 27001 certification), ensuring that risk mitigation is effectively integrated into the Company's overall risk management strategy.

9.3. Akeyless application security framework includes rigorous penetration testing to prevent unauthorized access to confidential information, with regular external tests and prompt resolution of critical issues. Akeyless also implements robust vulnerability management, conducting regular internal scans and quarterly production network scans, ensuring timely remediation of high-risk

vulnerabilities, including in source code as part of the SDLC. High or Critical issues are investigated and dealt with in accordance with Akeyless SDLC process or by any necessary means. Following that, a re-test is performed to verify the remediation of the relevant issues.

9.4. Patches are applied on an ongoing basis.

9.5. Akeyless will maintain a vulnerability management program that identifies and outlines the process for how vulnerabilities are managed for corporate systems along with Services provided to Customers.

9.6. Quarterly external network scans of the Services are conducted and monthly vulnerability test are conducted. Response time for known vulnerabilities are: critical [As soon as possible and no longer than 1 week from identification], high [No longer than 1 month from identification] medium [No longer than 3 months from identification] low [No longer than 3 months from identification]

9.7. Customer's will be notified through electronic means, or otherwise as stated in the Agreement, in the event of known and impacting vulnerabilities. Akeyless undertakes to prioritize the remediation of critical vulnerability confirmed to impact the Services or Customer Data.

10. Penetration Testing

10.1. An external web application penetration test is conducted on a regular basis.

10.2. Upon Customer's written request, Akeyless will share an executive summary report of the penetration test, or the results from the penetration test, in its sole discretion and subject to signed a non-disclosure agreement.

10.3. If required under applicable regulations (such as the EU DORA obligations on financial institutions), Akeyless will participate and cooperate with Customer's penetration testing requirements if and to the extend required under binding regulatory requirements or requested by a regulatory authority.

11. **Logging and Monitoring**

11.1. Akeyless will conduct log review through manual and automated processes. Akeyless will log critical information system activity. At a minimum, Akeyless systems shall record and retain the following audit logging information: activity was performed and by whom (credentials), status or outcome, failure vs success, time stamp and date.

11.2. Akeyless has implemented and will maintain a logging system aligned with industry standards to continuously monitor for unauthorized access, validation of the accuracy and integrity of received log events and will provide Customer the access logs to Customer's Account upon reasonable written request.

11.3. Akeyless has implemented and will maintain an intrusion detection and/or intrusion prevention systems, where appropriate and as reasonably necessary, with generated events fed into centralized systems for analysis.

11.4. Log data and logging systems will be maintained and configured to prevent changes or tampering of logs and will be kept for at least 12 months (or if required by applicable laws and jurisdictions, for 24 months).

11.5. Akeyless will implement and maintain specific technical controls to ensure non-repudiation of all log files, including limiting the number of administrators with access to logs and disabling administrator ability to delete or modify audit logs.

12. **Incident Response and Breach Notification**
    12.1. Akeyless will implement and maintain a tested Incident Response Plan (IRP), which will be managed and run by Akeyless' security team. Akeyless' security team will operate to a framework that includes incident management and breach notification policies and associated processes. Akeyless has an IRP which will include, at a minimum, preparation, detection, containment, investigation, remediation, and recovery.
    12.2. Akeyless will maintain an operational incident detection capability and a clearly documented incident response program for responding to suspected or known security incidents or system breaches.
    12.3. Akeyless requires personnel to report any known security incidents and Akeyless allocates considerable resources to ensure a secure code and infrastructure for all of its products. If you believe that you have found a vulnerability with respect to our security practices in any of our products, please report it to us immediately. Please be sure to include a brief description, including detailed steps that we can take in order to reproduce the issue and explain to us what the impact of such issue might be.
    12.4. In the event of an incident that affects Customer Data, Akeyless will utilize industry standard efforts to respond to the incident and mitigate the risk to Customer and Customer Data. Incident response plans must include methods to protect evidence of activity from modification and tampering.
    12.5. In the event of a confirmed security breach affecting Customer Data within Akeyless Services, and taking into account the scope of the Services provided by Akeyless, Akeyless will report to affected Customers an Incident Notification within 24-hours from becoming aware. For the purpose of this Policy, and Incident Notification includes (i) an assessment indicating the severity of the incident; (ii) the actual or approximate time at which the incident occurred; (iii) the actual or estimated location of the incident; (iv) the types and quantities of Customer Data affected; and (v) the measures Akeyless will take in order to mitigate the effects of the incident and the risk of repetition. In the event Akeyless does not have all the aforesaid information at time of notification, it will provide follow ups and updates upon becoming aware.
    12.6. Akeyless will reasonably cooperate with Customer in mitigation of the incident and in technical implementation.

13. **Business Continuity**
    13.1. Akeyless maintains a Business Continuity Plan ("**BCP**"), which defines the processes and procedures which need to be taken after an event, such as a natural disaster, that impacts the resources required to support the performance of its critical business processes. The BCP sets out necessary measures that need to be taken (and are taken by Akeyless) to ensure a continuous, undisturbed use of the Akeyless Services by Customers. The BCP is compliant with applicable standards and requirements, including regulations such as DORA and NIS2.
    13.2. Akeyless will test the effectiveness of its BCP on a regular basis, at least once per year as well as after implementation of a change with substantial impact on the BCP. The BCP was audited by an independent external auditor (during the SOC

and ISO annual audits, among others). Akeyless will provide a copy of such auditor report to its Customers, upon receiving reasonable written request.

13.3. Akeyless is committed to fix any issues that may rise regarding the BCP sufficiently effective, Akeyless shall remedy this ineffectiveness as soon as possible.

14. Disaster Recovery

14.1. Akeyless maintains backup policies and associated measures. Such backup policies include the constant monitoring of operational parameters, as relevant to the backup operations. Furthermore, the servers include an automated backup procedure.

14.2. Akeyless conducts regular checks with respect to the condition and labelling of data storage devices for data security. Akeyless ensures that regular tests are carried out to determine whether it is possible to undo the backup, as required and applicable.

14.3. Akeyless will create and maintain disaster recovery plans to restore customer-facing cloud products to customers. Disaster recovery plans will define Recovery Time Objectives ("**RTO**") and Recovery Point Objectives ("**RPO**") for the Services. RTO of the Customer Data: 1 hour, RPO of the Customer Data: 1 hour

15. Vendor Security and Management

15.1. Prior to the engaging with third party contractors, and sub-contractors (including sub-processors) (hereinafter, "**Subcontractors**") Akeyless performs are a reasonable due diligence check, including on such Subcontractors security standards, to ensure it complies with Akeyless' standard for data security protection. This may include a review of risk assessments, audits, and physical, technical, organizational, and administrative controls. Akeyless reviews its Subcontractors on an annual basis.

15.2. Any relevant Subcontractor is required to sign a data processing agreement, an information security exhibit and confidentiality provisions. The Subcontractor agreements, will include, where possible, audit rights, at least in the event of a security incident (conducted either by Akeyless, its Customer, or Supervisory Authority), an obligation to obtain a compliant business contingency plan and applicable service level commitments which comply with applicable laws.

15.3. Akeyless agrees to notify Customer of any change in the Subcontracting Chain that may have a material impact on the Services, such notification must be given in a timely manner, depending on the nature and impact of the development and on the applicable regulatory requirement. It is clarified, subject to the Agreement, notification on any change to the Subsector list available at: https://www.akeyless.io/list-of-sub-processors/ will be provided electronically by default (either by providing notice of such page, through the Account or by email, if and to the extent applicable). For the purpose of this Policy, a "Subcontracting Chain" will include all service providers, or ICT providers (as defined under DORA), that, directly or through Akeyless, provide all or a material part of the Service to the Customer, regardless of the data processing activities.

15.4. For more information, including the location of the Subcontractors, location of data processing please see Subcontractor list here: https://www.akeyless.io/list-of-sub-processors/

15.5. Notwithstanding the above, Akeyless is responsible for: (a) ensuring that the Service is provided by the Subcontracting Chain in compliance with the Agreement; and (b) ensuring that this compliance can be monitored in accordance with applicable laws and regulations.

16. Audit

16.1. Upon reasonable written notice and no more than once per year, Customers may request the latest copies of Akeyless's SOC 2 Report or ISO 27001/ ISO 27701, or other reports, such as penetration test or audit reports. All subject to a non-disclosure agreement or confidentiality obligations between Akeyless and Customer.

16.2. Akeyless undertakes to cooperate and respond to reasonable security audits, conducted through questionnaires or risk assessments provided by Customer.

16.3. Last, if required under applicable laws, or required by a regulator or authority, and to the extend the sections above do not satisfy Customer's or regulator's the inspection needs, and to the extent the parties contractually agreed, Akeyless will allow on-prem audits subject to: (a) prior written notice was provided; (b) the third party auditor is approved by Akeyless and the Customer ensures that whoever is performing the audit has appropriate and relevant skills and knowledge to perform the audit; (c) the audit shall be limited to solely the audit purposes and conducted solely during business hours; (d) the Customer undertakes to take extra care and not disrupt any operations during the audit; (e) will not be conducted more than once per year; and (f) all costs and expenses shall be fully paid by Customer.

17. Transfer Control

17.1. The parties confirm that the locations in the Agreement from where the Service is being provided or the location(s) where Customer Data is processed either by the Akeyless or by any of its Subcontractors, such locations will remain unchanged, except as otherwise agreed between the parties in the Agreement. Akyeless does not transfer any Customer Data outside of the Akeyless production environment.

17.2. Akeyless shall assess the risks related to the locations from where the Service is provided; and assess the risks, if applicable, related to the place where Akeyless and its subsidiaries are located.

18. Privacy and Data Protection

18.1. Akeyless confirms that it does not process any personal data on behalf of Customer, except as otherwise specified in the Agreement which is subject to the Akeyless DPA.

18.2. Akeyless shall comply with applicable laws and regulations, applicable to its Services, and shall adapt to any changes required under such laws.