AKKA

Lightbend Inc, d.b.a Akka

Resilience Guarantee Policy

February 21, 2025

Contents

1.1. Introduction

We believe in the resilience and reliability of Akka, to the point where we guarantee it.

We will indemnify against losses caused by an Akka application becoming unreliable in accordance with the terms of the agreement under which you purchase a subscription and/or license to use such Akka Application ("Your Agreement").

If Akka causes a loss of reliability in a customer's application, we will reimburse the customer for the period of unreliability in accordance with the terms and conditions set forth below and in Your Agreement.

1.2. Scope

This policy applies to a customer's use of Akka when licensed or subscribed for production use. If Your Agreement predates this policy, you should contact your account representative to update your agreement with us.

1.3. Referenced Policies

1. Cloud Services SLA Policy

1.4. Resilience Guarantee

1.4.1. Qualifying

In the event your Akka application becomes non-resilient, we will indemnify you against losses arising as a result of such non-resilience in accordance with the terms and conditions set forth in this document and in Your Agreement. To qualify for this indemnity:

- you must be an Akka customer in good standing with an enterprise subscription agreement that references this policy.
- your application must be using a version of Akka released within the last six (6) months prior to the qualifying event of non-resilience.
- your application must be running in production and must be authorized for use in a production environment.
- your application must be utilizing Akkas entity, persistence, and clustering features.

1.5. Claims

1.5.1. Filing a Claim

Assuming you qualify, to file a claim, you must open a support ticket via the Akka support portal within 72 hours of the application first exhibiting signs of non-resilient behavior.

The ticket should include:

- The unreliability time frame of your application, and
- either debug logs showing the unreliability events, or, a minimal reproducer that demonstrates the Akka core issue.

1.5.2. Validation

Your claim will be approved for remuneration after we have verified the issue causing the non-resilient behavior originates within Akka.

We will make every effort possible to validate the issue independently, however, we may require you to participate with us to diagnose the issue, including attempting suggested resolutions on a test system.

1.5.3. Limitations and Application of Credits

Once a claim is filed and validated, a reimbursement credit for 20 times the applicable license or subscription (as applicable) fee portion of the non-resilient period is issued.

This credit will be applied to future license or subscription (as applicable) fees with Akka and cannot be redeemed for cash or cash equivalent.

1.5.4. Exclusions

This guarantee does not apply to any unavailability, suspension or termination of Akka issues, directly or indirectly (the Exclusions):

- Caused by factors outside of Akka's reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Akka;
- That result from any actions or inactions of the customer, including failure to acknowledge a recovery volume or respond to resource health concerns;
- That result from equipment, software or other technology not supplied by Akka;
- Use of any pre-release of the Software such as Beta or Milestone releases, except for Developer Support and agreed to by Akka in an applicable Order Form;
- Use of software not obtained from Akka under the Support Agreement; or
- Arising from or during Akka's suspension or termination of your license or right to use Akka in accordance with Your Agreement. If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then Akka may, but is not required to, issue a Service Credit considering such factors.

1.6. Compliance

For Akka employees, failure to comply with this policy may result in progressive discipline up to and including dismissal. For non-Akka employees and contractors, failure to comply may result in removal of the individual's ability to access and use Akka data and systems. Employers of non-Akka employees will be notified of any violations.

Glossary

ISO/IEC 27001 Information technology - Security techniques - Information security management systems. 3

ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management controls. 3

ISO/IEC 27005 Information technology - Security techniques - Information security risk management. 3

ISO/IEC 27701 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and Guidelines. 3

Acceptable Risk Acceptable risk is the risk level that the management is prepared to accept as a business risk.. 3

ACL-DVS Assurance Life Cycle - Development Security. 3

AI Artificial Intelligence: Systems or applications that use machine learning algorithms, deep learning, natural language processing, or other techniques to perform tasks that typically require human intelligence.. 3

AI Risk Management Framework A structured approach to identifying, assessing, and mitigating risks associated with AI systems, as outlined by the NIST.. 3

AICPA American Institute of Certified Public Accountants. 3

Akka Data Any data stored on or originating from systems controlled by Akka for business purposes, including data that originates from Akka, Akka customers or data relating to Akka customers, excluding data classified as Public.. 3

Akka IT Members of Internal IT at Akka.. 3

ALC Assurance Life Cycle. 3

ALC-DES (Application Lifecycle) Delivery. 3

ALC-DLS (Application Lifecycle) Development Lifecycle. 3

ALC-DVS (Application Lifecycle) Development Security. 3

ALC-DVS.1.1.1C In the context of the EUCC (European Union Common Criteria) standard, ALC-DVS.1.1.1C is a specific assurance component within the Common Criteria framework. It falls under the ""ALC"" (Assurance Life Cycle) class, specifically the ""Development Security"" (DVS) family.. 3

ALC-DVS.2 A component of the Assurance Life Cycle (ALC) class within the Common Criteria (CC) framework (EUCC), specifically under the Development Security (DVS) family. This component requires that security measures in place during the development of the Target of Evaluation (TOE) are sufficient to protect the TOE and its associated assets. It aims to ensure that the development environment is secure and that the measures are adequate to maintain the confidentiality and integrity of the TOE throughout its development.. 3

Assets Entities that the owner of the TOE presumably places value upon. In the context of a Development Security System, assets are information in electronic or other form, information processing facilities and referring processes (incl. access control and alarm systems), development tools and environments, any manifestation of the TOE, and customer code and data provided to produce the TOE. 3

Assurance Classes Various assurance classes introduced and described in Part 3 of the Common Criteria.. 3

ATE Application Test. 3

Authentication Refers to the controls for providing Remote Users the means to verify or validate a claimed identity through the presentation of something they know (e.g., passwords), something they own (e.g., token), or something they are (e.g. fingerprint, biometrics, etc.).. 3

Authorization Refers to the controls for determining the resources that Remote Users are permitted to access based upon the permissions and privileges for which they have been authorized.. 3

Availability The property of being accessible and usable upon demand by an authorized entity. Business operations: General term for the entirety of operations performed by the developer related to the TOE, e.g. “personalization” is part of business operations.. 3

Business Continuity Planning Business Continuity Planning is concerned with keeping business operations running perhaps in another location or by using alternative tools and processes following a disaster.. 3

Business Impact Analysis Business Impact Analysis predicts the consequences of disruption of a business function, processes and gathers information needed to develop recovery strategies.. 3

C-SCRM Cybersecurity Supply Chain Risk Management. 3

can The word “can” is used for statements of possibility and capability, whether material, physical or causal. 3

CB Certification Body.. 3

CEM Common Evaluation Methodology.. 3

CFR Code of Federal Regulations (U.S.). 3

CISA The U.S. government’s Cybersecurity & Infrastructure Security Agency. 3

COBIT Control Objectives for Information and Related Technology. 3

Collector A business that buys, rents, gathers, obtains, receives, or accesses any personal information about a California resident by any means.. 3

Company Workstation A computing device owned by Akka and supplied to an Akka team member for use in performance of their job duties.. 3

Components A unit of software or hardware that can be both an entire system unto itself and used as part of a larger system. A component can be an entire operating system, a chip, an application, a package, a library, or even a single file or segment of source code. 3

Confidentiality The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.. 3

confidentiality and/or integrity The expression “confidentiality and/or integrity” means either “confidentiality” or “integrity”, or a combination of both. 3

CONOPS Concept of Operations. 3

Consent Consent of the Data Subject means any freely given, specific, informed, and unambiguous indication of the Data Subject’s wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.. 3

Consumer A natural person who is a California resident (CCPA). 3

Control Set of measures, associated to one or more objectives, intended to respond to threats.. 3

Controller The natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.. 3

COTS Common off-the-shelf. 3

cPP Common Criteria Collaborative Protection Profile, or just Collaborative Protection Profile (see https://www.commoncrite
3

CREF Common Criteria for SOC 2 (CREF). 3

CRM Customer Relationship Management. 3

Cross-Border Transfers Transfers of personal data from and to different establishments of the controller or processor, all located within the EU, or transfers of personal data from data subjects are in the different EU Member States to the controller or processor establishment which is based in an EU Member State. 3

CSF The NIST Cyber Security Framework (v2.0). 3

CSIRT Computer Security Incident Response Team. 3

CUI Controlled Unclassified Information. 3

CVE Common Vulnerabilities and Exposures. 3

CVRF Common Vulnerability Reporting Format. 3

CVSS Common Vulnerability Scoring System. 3

CWE Common Weakness Enumeration. 3

Data processing facilities Premises, equipment, installation or tool used for data processing. 3

Data Processing Register A record of processing activities that includes significant information about data processing, including data categories, the group of data subjects, the purpose of the processing and the data recipients. 3

Data Subject Request A request made by an individual or an individual's legal representative to request Akka to do something which falls under one of the rights granted to EU-based individuals by the GDPR.. 3

Data Subjects An identified or identifiable natural person.. 3

Deployer Any natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity. 3

Developer Entity (Site) offering services and being part of the development and production process; this encompasses all steps of the life cycle until delivery to the customer, e.g. software development, chip design, mask making, wafer production, testing, assembly etc. The developer is also responsible for supporting functions.. 3

Development environment Environment in which the TOE is developed; development includes the production of the TOE.. 3

Disaster Recovery Planning Disaster Recovery Planning is concerned with restoring normal business operations after a disaster takes place.. 3

DMZ Demilitarized Zone; in computer security, a DMZ is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet.. 3

DORA The EU Digital Operational Resilience Act. 3

DSD Development Security Documentation (EU CRA). 3

DSS Development Security System (EU CRA). 3

DT Data Treatment: Refers to how data is collected, processed, stored, and managed within a system or organization. It encompasses the procedures and practices involved in handling personal and sensitive data.. 3

DVS Development Security. 3

Employment The word 'employment' is meant here to cover all of the following different situations: employment of people (temporary or longer lasting), appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements.. 3

ENISA Agence européenne chargée de la sécurité des réseaux et de l'information, the European Union Agency for Cybersecurity. 3

EU CRA European Union Cyber Resiliency Act: The goal of the CRA is to protect consumers and strengthen the EU's overall level of resilience. This means reducing the risks for all users of digital products, whether private individuals or public entities — corporations, hospitals, banks, utilities, postal services and so on. The CRA is mandatory, and compliance is required for CE marking of regulated products, as well as for distribution in the European market. The CRA includes some strict, coercive measures such as heavy fines.. 3

EU DORA The EU Digital Operational Resilience Act. 3

EUCC European Union Common Criteria, a standard for evaluating the security of information technology products and systems, ensuring they meet defined security requirements and specifications. The EUCC framework is derived from the SOG-IS Common Criteria which in turn is based on the ISO/IEC 15408-1 Common Criteria standard for Information Technology Security Evaluation. However, the SOG-IS adds an additional layer of mutual recognition among European countries. This means that a product evaluated and certified in one member state under SOG-IS is recognized by other member states, reducing the need for multiple evaluations.. 3

Facility Any equipment, installation or tool, regardless of being software or hardware, which is part of the security management system.. 3

FIPS Federal Information Processing Standards (U.S.). 3

FW Firmware. 3

GRC Governance, Risk, Compliance. 3

High Security Area Area where TOE related data or material classified "critical" or "very critical" is accessible, and Security Control areas (access control and intrusion detection) where applicable.. 3

High-Risk AI AI systems that have significant implications for individuals' rights and freedoms, as defined under the EU AI Act.. 3

ICT Information and Communication Technology. 3

ICT Services Digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services. 3

ICT Third-Party Service Provider Any company (whether independent or part of a financial group) providing ICT services to financial entities. 3

IEC International Electrotechnical Commission, A global organization that prepares and publishes international standards for all electrical, electronic, and related technologies.. 3

Impact Impact (or consequence) refers to the extent to which a risk event might affect the organization.. 3

Incident Commander The person who acknowledges a reported incident. This is normally the person who is actively on-call.. 3

Information Security Event Any occurrence related to information assets or the environment indicating a possible compromise of policies, failure of controls, or an unmapped situation that can impact security.. 3

Information Security Incident A suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of information security policy.. 3

Inherent Risk The likelihood of an impact occurring when a threat compromises an unprotected asset. The current risk as it appears to the risk assessor before applying any control measures.. 3

Integrity The property of safeguarding the accuracy and completeness of assets.. 3

Intellectual Property Copyrights, trademarks, patents, and other information that is granted legal protections such as software.. 3

Internal Training Materials Media and content that you use to train your employees and partners.. 3

International data transfers Cross border flows of personal data from a Member State of the European Economic Area (the EU Member States and Liechtenstein, Iceland, and Norway) to a third country or international organization, as well as further transfers from that third country or organization to another country. 3

IP Intellectual Property (sometimes in technical context also Internet Protocol). 3

IS Information security - Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.. 3

IS event An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.. 3

IS Incident An Information Security (IS) incident. A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.. 3

ISMS Information Security Management System. 3

ISO International Organization for Standardization. It is an independent, non-governmental international organization that develops and publishes standards to ensure the quality, safety, efficiency, and interoperability of products, services, and systems. 3

ITIL Information Technology Infrastructure Library. 3

ITSEF ITSEF stands for Information Technology Security Evaluation Facility. It is an accredited laboratory responsible for conducting security evaluations of IT products and systems according to the Common Criteria standards. 3

JIL Joint Interpretation Library. 3

Likelihood How often the risk event might happen (e.g., per procedure/episode or within a specified timeframe).. 3

Malicious Code Virus, worms, Trojans, spyware and adware based on the perceived intent of the author.. 3

may Indicates a course of action permissible within the limits of the document. 3

Mobile Code Software obtained from remote systems transferred across the network, e.g. Java code, activeX controls, flash animations, office macros etc.. 3

NIST The U.S. National Institute of Standards and Technology, a U.S. federal government agency that develops technical standards, guidelines, and best practices in various fields, including cybersecurity, cryptography, and information technology as a part of the U.S. Department of Commerce. 3

OS Operating System. 3

OWASP Open Web Application Security Project. 3

Personal Device A device not owned by Akka, but owned by a User. Examples include personal cell phones, tablets, smart watches and so forth.. 3

Personal Information Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. (e.g., direct identifiers (real name, alias, postal address, social security numbers, driver's license, etc.), Indirect identifiers (cookies, IP addresses, account name, etc.), Biometric data, Internet activity, etc. See Personal Data.. 3

Remote Access Credentials Refers to identification and authentication credentials/data such as User IDs, passwords, tokens, etc.. 3

Remote Access Systems Refers to the systems, networks, and applications that facilitate remote access to Company information and systems.. 3

Sensitive Information Refers to information that is classified as other than Public.. 3

shall Indicates measures strictly to be followed in order to conform to the document and from which no deviation is permitted. 3

should Indicates that among several possibilities, one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required. The CC interpret "not necessarily required" to mean that the choice of another possibility requires a justification of why the preferred option was not chosen. 3

TOE Target of Evaluation: Refers to the specific product, service, or system that is being assessed for cybersecurity compliance.. 3

Two-Factor Authentication Refers to the method of authentication that requires two factors before a Remote User will be allowed access to a network or system: a hardware or software token that produces a code that will change randomly at short time intervals and a password which is unique and only valid for the token.. 3

Vulnerability A weakness that could permit a threat to compromise the security of information assets.. 3

Index