AKKA

Lightbend Inc, d.b.a Akka

Customer Support Policy

July 15, 2025

Contents

1.1. Introduction

Akka provides Customer Support to support its customers. This policy covers Akka products that are deployed, managed, and hosted by the customer in their own environment, as well as those that are hosted or managed by Akka.

The Customer Support policy is designed to ensure that all customers receive prompt, professional, and courteous support. This policy provides an overview of the support and maintenance policies, which are part of the Akka Subscription and Product worldwide offerings.

1.2. Scope

This policy applies to all customers participating in Akkas Subscription Plans and applies to all employees and contractors who deal with customers. Akkas goal is to ensure the success of each customer. Customers may use Akka Support to ask questions in addition to reporting bugs. Akka Support will guide the use of Akka technologies. Support does not include code or architectural reviews in-depth, nor does it include writing any application code. For services like these, the customer can engage Akkas Professional Services team.

1.3. Referenced Policies

1. Disciplinary Policy
2. Incident Management Policy

1.4. Referenced Frameworks and Standards

1. AICPA System Organization and Controls 2

1.5. Customer Support

We support our customers using our products.

1.5.1. Customer Support System

We provide a support system that allows users to report suspected defects, complaints, issues, and any other challenge through an appropriate channel.

Reported tickets are addressed by our support staff in a timely manner, as detailed in this policy.

1.6. Product

Our policies around how our products are supported.

1.6.1. Product Support Policy

We support all of our products that have not been designated as end-of-life, meaning we will provide support services as described in this policy.

We proactively fix discovered CVEs and bugs only in the latest version, not previous versions.

Customers may request remediation for CVEs on all supported versions. Akka will advise if remediation will be included in an existing version (via a patch version release) or if it will require an upgrade.

1.6.2. New Versions

Whenever a new version of a product is released (including minor patch versions), the product becomes supported. This support is available on that version for a period of two years from the release date of that version, at a minimum.

1.6.3. End-of-Life Notice

In the event we plan to end-of-life a product or module, we will provide a minimum of two (2) years notice.

1.7. Support Levels

Defining the different levels of support are provided.

1.7.1. Support Classifications

Akka offers 24/7, Developer, and Basic support. 24/7 Support satisfies the requirements of deployed production applications while Developer support assists during the development of the application:

Support	Description	Subscription Type
24/7	24/7 support is geared towards enterprise customers who require around-the-clock support. This option provides customers with 24 hours per day, 7 days per week, and 365 days per year coverage for production outages (Severity 1). 24/7 support is ideal for mission-critical applications. To expedite a response, the case must be opened as a Severity 1 or 2 in the Support Portal making sure that it falls under the definition of Severity 1 or 2 as set forth in Section 3.2.	Enterprise, Serverless-Critical, Serverless-Priority, Bring Your Own Cloud, Self Hosted
Developer	Developer support is for assistance during the development phase of an application. Developer support is not for production systems. Severity 1 and 2 are not applicable to Developer support (as they are only for systems in production)	ISV/OEM, Growth
Basic	Basic support is equivalent to Developer supportassisting during the development phase of an application and not intended for production systems but provided at a lower SLO.	Academic, Dev Subscription, Startup, Serverless-Explorer

The number of support incidents is unlimited for all classifications.

Support Contact Information

- Email: support@akka.io
- Website: https://support.akka.io

1.7.2. Severity Levels

Incident severity levels are a measurement of the impact an incident has on the business.

Severity	Description	Akka Response
Severity 1	An Error in the Software which severely affects the overall production performance of the Softwares function or process, such that a production system is non-functional and no procedural workaround exists. *Only applicable to production environments.*	Akka will work continuously on Severity 1 incidents until a workaround or system recovery is successfully implemented and either the incident is closed or the severity is reduced. When required, Akka will provide a patch release to resolve Severity 1 incidents
Severity 2	An Error in the Software which materially affects the overall production performance of the Softwares function or process so that the function or process is noticeably impaired, but where business operations continue. *Only applicable to production environments.*	Akka will work to provide a resolution to Severity 2 incidents by a reasonable date agreed to between Akka and the Customer. When required Akka will provide a patch release to resolve Severity 2 incidents.

Severity 3	An Error that does not materially affect the overall performance of a production function or process. This may include a minor issue with limited loss or no loss of functionality or impact on the Customer's operations. Also an Error in a non-production environment which is requested to be reviewed at a higher priority due to it blocking critical development efforts.	Akka will work to provide a resolution to Severity 3 incidents in an Upgrade release.
Severity 4	An Error encountered in a non-production environment, general usage questions, and documentation Errors.	Akka will work to provide a resolution to Developer incidents in an Upgrade release.

1.8. Support Classifications

How support services are classified and how those classifications are applied.

1.8.1. Policy

Akka is committed to providing the best possible support to all our customers. Akka strives to resolve all customer queries and requests as soon as possible and to keep our customers informed throughout the process.

Customers with Akka subscriptions will get support and access to the Customer Portal where the customer may submit support cases and view the Akka knowledge base, security alerts, documentation, and other technical content.

All support interactions will be conducted in English.

Support cases may be submitted for experimental features, however, the expected response times below do not apply in this case.

1.9. Response Times

Expected response times for support services.

1.9.1. Response Times

For customer support for products/services not hosted by Akka, Akka will use commercially reasonable efforts to provide an acknowledgment of a reported Issue to the Customer and respond within the target time frames specified below (Response Time). Response times define the maximum time to initially respond to the customers report of an incident, the time for a workaround or patch, and the time for a permanent correction to the incident, if applicable.

While not making a guarantee or warranty, Akka will make commercially reasonable efforts to respond to Error reports within the timeframes outlined in the tables below for each Support level.

24/7

Severity	**Target Response Time**	**Target Work Around Time**	**Target Permanent Correction Time**
Severity 1	1 hour, any time of day (24 x 7 x 365)	3 hours	Next Release
Severity 2	4 business hours	1 business day	Next Release
Severity 3	1 business day	Future Release	Future Release
Severity 4	1 business day	Future Release	Future Release

To expedite a response, the case must be opened as a Severity 1 or 2 in the Support Portal making sure that it falls under the definition of Severity 1 or 2 as set forth in Section 3.2; these instructions must be followed to expect the noted response time.

Because there are fixed times during which an incident can be reported, the response time shown is not necessarily contiguous. For example, if an incident is reported at 5:00 PM on a Friday afternoon, it may be as late as the following Monday morning before a response is issued.

Developer

Severity	Target Response Time	Target Work Around Time	Target Permanent Correction Time
Severity 4	1 business day	Future Release	Future Release

Because there are fixed times during which an incident can be reported, the response time shown is not necessarily contiguous. For example, if an incident is reported at 5:00 PM on a Friday afternoon, it may be as late as the following Monday morning before a response is issued.

Basic

Severity	Target Response Time	Target Work Around Time	Target Permanent Correction Time
Severity 4	3 business days	Future Release	Future Release

Because there are fixed times during which an incident can be reported, the response time shown is not necessarily contiguous. For example, if an incident is reported at 5:00 PM on a Friday afternoon, it may be as late as the following Monday morning before a response is issued.

1.9.2. Support Availability

Akka provides support to customers worldwide. Each customer will be designated a regional support center that best matches the customers time zone. Response times are dictated by the time zone of the customers designated support center. Support hours are **08:00 to 18:00, Monday through Friday**, within the time zone of the designated regional support center. Daylight savings time changes apply within each centers time zone. Holidays are regional and are itemized below. Akka provides support in the following support centers:

Support Center	Time Zone Holidays	
Australia	Australian Eastern Time (AET)	New Year's Day, Australia Day, Good Friday, Easter Monday, Anzac Day, Queens Birthday, Labour Day, Christmas Day, Boxing Day.
Central Europe	Central European Time (CET)	New Year's Day, St Berchtold, Good Friday, Easter Monday, Ascension, Whit Monday, Swiss National Day, Federal Fast holiday, Christmas Day.
US East	Eastern Time (EST)	New Year's Day, Martin Luther King Day, Presidents Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, Day after Thanksgiving, and Christmas Day.
US Pacific	Pacific Time (PST)	New Year's Day, Martin Luther King Day, Presidents Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, Day after Thanksgiving, and Christmas Day.

1.10. 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 individuals 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. 5

ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management controls. 5

ISO/IEC 27005 Information technology - Security techniques - Information security risk management. 5

ISO/IEC 27701 Security techniques Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management Requirements and Guidelines. 5

Acceptable Risk Acceptable risk is the risk level that the management is prepared to accept as a business risk.. 5

Access Control Means to ensure that physical and logical access to Assets is authorized and restricted based on business and information security requirements. 5

ACL-DVS Assurance Life Cycle - Development Security. 5

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.. 5

AI Risk Management Framework A structured approach to identifying, assessing, and mitigating risks associated with AI systems, as outlined by the NIST.. 5

AICPA American Institute of Certified Public Accountants. 5

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.. 5

Akka IT Members of Internal IT at Akka.. 5

ALC Assurance Life Cycle. 5

ALC-DES (Application Lifecycle) Delivery. 5

ALC-DLS (Application Lifecycle) Development Lifecycle. 5

ALC-DVS (Application Lifecycle) Development Security. 5

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.. 5

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.. 5

Asset See Asset. 5

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. 5

Assurance Classes Various assurance classes introduced and described in Part 3 of the Common Criteria.. 5

ATE Application Test. 5

Attack successful or unsuccessful unauthorized attempt to destroy, alter, disable,gain access to an Asset or any attempt to expose, steal, or make unauthorized use of an Asset. 5

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.).. 5

Authenticity Property that an Entity is what it claims to be.. 5

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.. 5

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.. 5

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.. 5

Business Impact Analysis Business Impact Analysis predicts the consequences of disruption of a business function, processes and gathers information needed to develop recovery strategies.. 5

C-SCRM Cybersecurity Supply Chain Risk Management. 5

can The word can is used for statements of possibility and capability, whether material, physical or causal. 5

CB Certification Body.. 5

CEM Common Evaluation Methodology.. 5

CFR Code of Federal Regulations (U.S.). 5

Chain of Custody Demonstrable possession, movement, handling and location of material from one point in time until another.. 5

CISA The U.S. government's Cybersecurity & Infrastructure Security Agency. 5

COBIT Control Objectives for Information and Related Technology. 5

Collector A business that buys, rents, gathers, obtains, receives, or accesses any personal information about a California resident by any means.. 5

Company Workstation A computing device owned by Akka and supplied to an Akka team member for use in performance of their job duties.. 5

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. 5

Confidentiality The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.. 5

confidentiality and/or integrity The expression confidentiality and/or integrity means either confidentiality or integrity, or a combination of both. 5

CONOPS Concept of Operations. 5

Consent Consent of the Data Subject means any freely given, specific, informed, and unambiguous indication of the Data Subjects 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.. 5

Consumer A natural person who is a California resident (CCPA). 5

Control Set of measures, associated to one or more objectives, intended to respond to threats. Measure that maintains and/or modifies risk.. 5

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.. 5

COTS Common off-the-shelf. 5

cPP Common Criteria Collaborative Protection Profile, or just Collaborative Protection Profile (see https://www.commoncriteriaportal.org/index.cfm). 5

CREF Common Criteria for SOC 2 (CREF). 5

CRM Customer Relationship Management. 5

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. 5

CSF The NIST Cyber Security Framework (v2.0). 5

CSIRT Computer Security Incident Response Team. 5

CUI Controlled Unclassified Information. 5

CVE Common Vulnerabilities and Exposures. 5

CVRF Common Vulnerability Reporting Format. 5

CVSS Common Vulnerability Scoring System. 5

CWE Common Weakness Enumeration. 5

Data processing facilities Premises, equipment, installation or tool used for data processing. 5

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. 5

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.. 5

Data Subjects An identified or identifiable natural person.. 5

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. 5

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.. 5

Development environment Environment in which the TOE is developed; development includes the production of the TOE.. 5

Disaster Recovery Planning Disaster Recovery Planning is concerned with restoring normal business operations after a disaster takes place.. 5

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.. 5

DORA The EU Digital Operational Resilience Act. 5

DSD Development Security Documentation (EU CRA). 5

DSS Development Security System (EU CRA). 5

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.. 5

DVS Development Security. 5

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.. 5

ENISA Agence européenne chargée de la sécurité des réseaux et de l'information, the European Union Agency for Cybersecurity. 5

Entity Item relevant for the purpose of operation of a domain that has recognizably distinct existence.. 5

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.. 5

EU DORA The EU Digital Operational Resilience Act. 5

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.. 5

Facility Any equipment, installation or tool, regardless of being software or hardware, which is part of the security management system.. 5

FIPS Federal Information Processing Standards (U.S.). 5

FW Firmware. 5

GRC Governance, Risk, Compliance. 5

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.. 5

High-Risk AI AI systems that have significant implications for individuals' rights and freedoms, as defined under the EU AI Act.. 5

ICT Information and Communication Technology. 5

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. 5

ICT Third-Party Service Provider Any company (whether independent or part of a financial group) providing ICT services to financial entities. 5

IEC International Electrotechnical Commission, A global organization that prepares and publishes international standards for all electrical, electronic, and related technologies.. 5

Impact Impact (or consequence) refers to the extent to which a risk event might affect the organization.. 5

Incident An unplanned interruption or reduction in quality of service or breach of our Cloud Services SLA Policy, or any event that requires an immediate and time-sensitive response in order to avoid security or availability issues for our customers.. 5

Incident Bridge The means of live communication with anybody investigating the Incident. It will be ensured to be accessible by the Incident reporter, also.. 5

Incident Commander The person actively responsible for managing and resolving the Incident. They retain that role until an explicit hand off is made.. 5

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.. 5

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.. 5

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.. 5

Integrity The property of safeguarding the accuracy and completeness of assets.. 5

Intellectual Property Copyrights, trademarks, patents, and other information that is granted legal protections such as software.. 5

Internal Training Materials Media and content that you use to train your employees and partners.. 5

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. 5

IP Intellectual Property (sometimes in technical context also Internet Protocol). 5

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.. 5

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.. 5

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.. 5

ISMS Information Security Management System. 5

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. 5

ITIL Information Technology Infrastructure Library. 5

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. 5

JIL Joint Interpretation Library. 5

Likelihood How often the risk event might happen (e.g., per procedure/episode or within a specified timeframe).. 5

Malicious Code Virus, worms, Trojans, spyware and adware based on the perceived intent of the author.. 5

may Indicates a course of action permissible within the limits of the document. 5

Mobile Code Software obtained from remote systems transferred across the network, e.g. Java code, activeX controls, flash animations, office macros etc.. 5

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. 5

OS Operating System. 5

OWASP Open Web Application Security Project. 5

Personal Device A device not owned by Akka, but owned by a User. Examples include personal cell phones, tablets, smart watches and so forth.. 5

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.. 5

Remote Access Credentials Refers to identification and authentication credentials/data such as User IDs, passwords, tokens, etc.. 5

Remote Access Systems Refers to the systems, networks, and applications that facilitate remote access to Company information and systems.. 5

Sensitive Information Refers to information that is classified as other than Public.. 5

shall Indicates measures strictly to be followed in order to conform to the document and from which no deviation is permitted. 5

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. 5

TOE Target of Evaluation: Refers to the specific product, service, or system that is being assessed for cybersecurity compliance.. 5

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.. 5

Vulnerability A weakness that could permit a threat to compromise the security of information assets.. 5

Index