



Axiad Cloud Services Agreement

This Axiad Cloud Services Agreement is between the entity you represent, or, if you do not designate an entity in connection with a Subscription purchase or renewal, you individually ("Licensee"), and Axiad IDS, Inc. ("Axiad"). It consists of the terms and conditions below, as well as the Online Services Terms, the SLAs (Exhibit A), and the Offer Details for your Subscription or renewal (together, the "agreement"). It is effective on the date we provide you with confirmation of your Subscription or the date on which your Subscription is renewed.

1. DEFINITIONS

- 1.1 "Confidential Information" means non-public information a party disclosed by such party to the other party pursuant to this Agreement. Confidential Information of Customer includes Account Information and Customer Data, and Confidential Information of Axiad includes the Services and related documentation, technology and pricing.
- 1.2 "Customer Data" has the meaning specified in Section 5.1.
- 1.3 "Consulting Services" means implementation, customization or other services provided by Axiad to Customer other than Axiad's standard Services, as such other services are described in a Schedule executed by the parties.
- 1.4 "Customer Security Procedures" has the meaning specified in Section 2.1.
- 1.5 "Documentation" means the documentation Axiad makes available to Customer as part of the Services, including URLs for websites, technical information, policies or terms contained in or linked to by webpages or applications associated with the Services, as updated by Axiad from time to time.
- 1.6 "Hardware" means the hardware products used in connection with the Services, such as readers, access cards, printers, consumables and devices, which are identified on the applicable Purchase Order.
- 1.7 "Purchase Order" means an ordering document executed by Customer and Axiad or a Related Party indicating the type, usage parameters, fees and other details regarding the Services and any related Consulting Services to be provided by Axiad or a Related Party in accordance with this Agreement.
- 1.8 "Related Party" means an Axiad reseller or an Axiad affiliate, as specified on the applicable the Purchase Order.
- 1.9 "Schedule" means an attachment that expressly incorporates this Agreement by reference and is executed by Axiad or the Related Party and the Customer (e.g. Statements of Work, Purchase Orders). For clarity, each Schedule is incorporated in and becomes part of this Agreement upon the execution of such Schedule by Axiad and the Customer.



- 1.10 "Security Procedures" has the meaning specified in Section 2.1.1.
- 1.11 "Online Services" or "Services" means Axiad-hosted services for issuing and managing identity credentials, which services are identified on the applicable Purchase Order.
- 1.12 "Service Levels" has the meaning specified in Section 2.1.1.
- 1.13 "Third Party Service" means a service developed or licensed by a third party and hosted by Axiad as part of the Services, which service is identified on the applicable Purchase Order.
- 1.14 "Users" means natural persons who are authorized by Customer to use the Service, and who have been supplied user identifications by Customer (or by Axiad at Customer's request). Users may include Customer employees, consultants, contractors and agents, provided that any consultants and contractors have agreed in writing to comply with the terms of this Agreement.
- 1.15 "User Portal" means the Axiad Cloud web page that is accessed by Customer End User to add, view or manage their Identity Credentials
- 1.16 "Operator Portal" means the Axiad Cloud web page that is available to Customer IT administrators or operators to perform management related tasks such as issuing credentials to users, troubleshooting or reviewing audit logs.
- 1.17 "Enrollment Service" means Axiad Cloud APIs that are available for requesting and retrieving PKI credentials.

2. PROVISION AND USE OF SERVICES

2.1 Axiad Responsibilities.



2.1.1 Axiad will use reasonable efforts to make the Services available in accordance with the metrics set forth on Exhibit A (the “Service Levels”), the security practices set forth on Exhibit B (the “Information Security”), and otherwise in accordance with this Agreement.

2.1.2 Axiad will operate and maintain Axiad software and other infrastructure owned or leased by Axiad and used to provide the Services (“Axiad Infrastructure”), including the implementation of updates and upgrades to Axiad Infrastructure. Unless otherwise specified on the Purchase Order or Schedule, Axiad will make available to Customer as necessary for it to receive the Services the most up-to-date version of Axiad Infrastructure that Axiad makes generally commercially available.

2.1.1 If Axiad and Customer agree on the provision of any Consulting Services in connection with the Services, such Consulting Services shall be set forth in a separate Schedule executed by the parties. Axiad will provide such Consulting Services in accordance with such Schedule.

2.2 Right to Use Services. Subject to the terms and conditions of this Agreement, Axiad grants Customer the right to access and use Axiad Infrastructure as necessary to receive the Services in accordance with the terms set forth on the applicable Purchase Order (e.g., number of Users, applicable Hardware) and in accordance with the applicable Documentation.

2.3 Customer Responsibilities. Customer agrees to do the following in connection with its use of the Services: (i) comply with all applicable laws, rules and regulations, including those regarding data privacy and export control; (ii) use reasonable security precautions for providing access to the Services and associated data by its employees or other individuals to whom Customer provides access including passwords, private keys, service accounts and other sensitive data; (iii) cooperate with Axiad’s reasonable investigation of outages, security problems, and any suspected breach of this Agreement; (iv) give Axiad true, accurate, current, and complete information (“Account Information”) when establishing Customer’s account associated with the Services; (v) keep Customer’s billing contact and other Account Information up to date; (vi) be responsible for the use of the Services by Customer, and any person to whom Customer has given access to the Content or Services, and any person who gains access to Customer’s Content or the Services; (vii) notify Axiad of any known or suspected unauthorized use of Customer’s account, the Services, or any other breach of security; (viii) not store or transmit via the Services any content (including Customer Data) that infringes or otherwise violates the rights of a third party; (ix) not use the Services where failure or fault of the Services could lead to death or serious bodily injury of any person or to physical or environmental damage; and (x) not disclose or provide access to the Services, the Documentation, or any other information provided by Axiad to Customer hereunder to any third party except as expressly permitted herein.

2.4 Suspension and Changes to the Services. Axiad may suspend provision of the Services if: (i) Axiad reasonably believes that the Services are being used by Customer in violation of this Agreement or any law; (ii) Customer does not cooperate with Axiad’s investigation of any suspected violation of this Agreement or any investigation by a government authority; (iii) Axiad reasonably believes that suspension of the Services is necessary to protect Axiad’s network, Axiad’s other customers, or others in general; (iv) a payment for the Services is overdue by more than thirty (30) days or (v) suspension is required by law. Axiad will use reasonable efforts to give Customer advance notice of a suspension under this Section 2.4.

3. FEES AND PAYMENTS

- 3.1 Invoicing and Payment. Customer agrees to pay the fees specified on the applicable Purchase Order (the “Fees”) to Axiad or the Related Party specified on the PO. Unless otherwise specified on the applicable Purchase Order, Customer shall pay all Fees within thirty (30) days after the date of the invoice for such Fees.
- 3.2 Taxes. The Fees do not include any direct or indirect local, state, federal or foreign taxes, levies, duties or similar governmental assessments of any nature, including value-added use or withholding taxes (collectively, “Taxes”). Customer is responsible for paying all Taxes associated with its use of Services, excluding taxes based solely on Axiad’s or the applicable Related Party’s net income. If Axiad or the applicable Related Party has the legal obligation to pay or collect Taxes for which Customer is responsible under this Section 3.2, the appropriate amount shall be invoiced to and paid by Customer, unless Customer provides Axiad or the applicable Related Party with a valid tax exemption certificate authorized by the appropriate taxing authority.

4. WARRANTY

- 4.1 Service Warranty. Axiad warrants that it will use reasonable efforts to perform the Services in accordance with this Agreement and otherwise in a good and workmanlike manner, and that Axiad will implement reasonable measures to detect and mitigate the effects of any viruses and other malicious code discovered on the systems that provide the Services. For clarity, Axiad does not provide any warranty or other services with respect to the Hardware, and Customer is responsible for obtaining and enforcing any warranty or service obligations with respect to the Hardware.
- 4.2 Disclaimer. EXCEPT AS SPECIFIED IN SECTION 4.1, AXIAD MAKES NO WARRANTIES OR REPRESENTATIONS REGARDING THE SERVICES OR OTHERWISE UNDER THIS AGREEMENT, AND AXIAD HEREBY DISCLAIMS ANY OTHER EXPRESS OR IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR PARTICULAR PURPOSE.

5. CUSTOMER DATA AND IP OWNERSHIP

- 5.1 Customer Data. Customer shall own all right, title and interest in any and all data and content that Customer submits via the Services, including any Account Information (collectively, “Customer Data”). Axiad shall implement the Security Procedures to protect the Customer Data from unauthorized disclosure. Customer hereby grants Axiad a non-exclusive license to use the Customer Data to perform the Services. Customer shall not submit as Customer Data any personal or other information that is not necessary for the receipt of the Services (e.g., protected health information, bank account information) and Axiad shall not have any obligation, responsibility or liability with respect to any such information that is submitted via the Services or otherwise provided to Axiad.



5.2 Axiad IP. Axiad shall own and retain all right, title and interest in, the Services, the Documentation, and any related software or systems used to provide the Services (including the Axiad Infrastructure), any work product generated as a result of any Consulting Services, and all proprietary rights in the foregoing (collectively, “Axiad IP”). Axiad hereby grants Customer a non-exclusive license to use Axiad IP during the term of this Agreement as necessary to receive the Services.

5.3 Customer Data retention.

- Axiad will retain all customer & service data for a maximum of up to 2 years during the lifetime of this contract.
- If requested by the customer, the data will be available to the customer 45 days from when the customer submits a written request, during the lifetime of this contract.
- Axiad’s retention of customer data is purely for Axiad’s consumption, and should not be relied upon to meet any compliance, or other needs that the customer may have.
- The customer will be provided audit events from CMS, PKI, and Authentication data, and it is the customer’s responsibility to retain and manage their data in accordance with their security, compliance or any other needs.
- Upon termination of this contract, all customer data stored in Axiad Cloud will be deleted.

6. CONFIDENTIALITY

- 6.1 Any Confidential Information of the disclosing party is and shall remain the exclusive property of such party or, as the case may be, third parties who have entrusted the processing of such information to such party.
- 6.2 The receiving party and its contractors may only use and disclose the Confidential information of the disclosing party to perform its obligations or exercise its rights set forth herein. The receiving party shall protect the Confidential Information from disclosure to third parties (other than advisors and contractors who require it in order to fulfill their obligations) in the same manner the receiving party protects its own similar confidential information. The receiving party shall require its advisors and contractors to whom it makes Confidential Information of the disclosing party available as permitted hereunder to abide by this confidentiality undertaking.
- 6.3 The receiving party shall not have any confidentiality obligation with respect to any Confidential Information of the disclosing party:



- 6.3.1 Which is disclosed to the receiving party by a third party which has no confidentiality obligation toward the disclosing party or a third party;
 - 6.3.2 Which at the time of its disclosure is in the public domain or comes into the public domain thereafter, other than due to the breach of contractual or legal obligations of a third party, of which the receiving party is aware, or of the receiving party;
 - 6.3.3 Which must be disclosed by law or court order; of which the receiving party is already aware, without a confidentiality obligation, and for which it can provide written or other reasonable evidence proving such prior knowledge.
- 6.4 If the receiving party is required by law or court order to disclose any Confidential Information of the disclosing party, it shall notify the disclosing party thereof upon receipt of the notice, proceedings or order in order to allow it to contest the proceedings or order, limit the content and scope of the disclosure or obtain an order to protect the Confidential Information. The Parties agree to cooperate with each other for such purpose.

7. LIMITATION OF LIABILITY

IN NO EVENT WILL AXIAD'S AGGREGATE LIABILITY FOR DAMAGES UNDER THIS AGREEMENT EXCEED THE AMOUNT CUSTOMER PAID TO AXIAD UNDER THIS AGREEMENT FOR THE SERVICES THAT GAVE RISE TO THE CLAIM DURING THE TWELVE (12) MONTHS PRECEDING THE INITIAL CLAIM FOR WHICH A PARTY RECOVERS DAMAGES HEREUNDER. NEITHER PARTY WILL HAVE ANY OBLIGATION OR LIABILITY TO THE OTHER (WHETHER ARISING IN CONTRACT, WARRANTY, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE) FOR ANY INCIDENTAL, INDIRECT, PUNITIVE, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LIABILITIES (INCLUDING LOST PROFITS), EVEN IF SUCH PARTY IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LIABILITIES, ARISING FROM OR RELATED TO THIS AGREEMENT.

8. TERM AND TERMINATION

- 8.1 Term of Agreement. The term of this Agreement shall commence on the Effective Date and shall continue for the term specified on the signed Purchase Order for the period of twelve (12) months (with respect to the Services described on such Purchase Order).
- 8.2 Termination for Convenience. Customer may terminate this Agreement for convenience at any time. If Customer terminates this Agreement for convenience, Customer shall pay Axiad all amounts then due or that would be due within thirty (30) days after such termination. For clarity, Axiad will have no obligation to refund any fees to Customer in connection with any such termination.
- 8.3 Termination for Breach. Either party may terminate this Agreement for breach upon written notice to the other party if the other party materially breaches this Agreement and does not remedy such breach within thirty (30) days after its receipt of a written notice from the non-breaching party describing such breach.
- 8.4 Effect of Termination. Customer shall discontinue use of the Services, including relinquishing the use of any materials (including any software or Documentation) provided to Customer by Axiad in connection with the Services, and all licenses and other rights granted by Axiad to Customer hereunder shall terminate. Axiad will have no obligation to provide any transition services or access to data except as stated in Section 8.5.
- 8.5 Transition Assistance. Upon Customer's request, Axiad and Customer shall enter a Schedule describing Consulting Services necessary to assist Customer in retrieving Customer Data and other Customer Confidential Information in connection with any termination or expiration of this Agreement.

9. GOVERNING LAWS AND NOTICES

- 9.1 Jurisdiction. This Agreement is governed by the laws of the State of California, exclusive of any choice of law principle that would require the application of the law of a different jurisdiction. This Agreement shall not be governed by the United Nations Convention on the International Sale of Goods. Exclusive venue for all disputes arising out of this Agreement shall be in the state or federal courts in Santa Clara, California and the parties each agree not to bring an action in any other venue. Customer waives all objections to this venue and agrees not to dispute personal jurisdiction or venue in these courts, provided that either party may bring a claim for preliminary injunctive or other preliminary relief in any jurisdiction to enforce its rights under this Agreement. Each party agrees that it will not bring a claim under this Agreement more than two years after the time that the claim accrued.
- 9.2 Assignment. Customer may not assign this Agreement without Axiad's prior written consent, and any attempted assignment in violation of the foregoing shall be null and void. Axiad may assign this agreement to an affiliate or to a successor to all or substantially all of Axiad's business that relates to this agreement.



- 9.3 Severability. If any provision in this Agreement is held invalid or unenforceable by a body of competent jurisdiction, such provision will be construed, limited or, if necessary, severed to the extent necessary to eliminate such invalidity or unenforceability. The remaining provisions of this Agreement will remain in full force and effect.
- 9.4 No waiver. Axiad's failure to exercise or delay in exercising any of its rights under this Agreement will not constitute a waiver, forfeiture, or modification of such rights. Axiad's waiver of any right under this Agreement will not constitute a waiver of any other right under this Agreement or of the same right on another occasion. Axiad's waiver of any right under this Agreement must be in writing.
- 9.5 Force Majeure. Axiad will not be in violation of this Agreement if the failure to perform the obligation is due to an event beyond Axiad's control, such as significant failure of a part of the power grid, general failure of the Internet, natural disaster, war, riot, insurrection, epidemic, strikes or other organized labor action, terrorism, or other events beyond Axiad's control, including acts or omissions by Customer that prevent or inhibit Axiad's performance of the Services.
- 9.6 Relationship of the Parties. The parties' relationship is that of independent contractors and not business partners. Neither of the parties is the agent for the other, and neither party has the right to bind the other on any agreement with a third party.
- 9.7 Notices. The parties may exchange routine operational communications regarding the Services via an electronic means designated by Axiad. Notices regarding breaches of this Agreement, indemnification, or other non-routine legal matter matters, shall be sent by a nationally recognized overnight courier to the address for the recipient party specified at the beginning of this Agreement (or other address provided by such party in writing). All notices must be given in the English language.
- 9.8 Entire Agreement. This Agreement constitutes the entire understanding and agreement between Customer and Axiad and supersedes all prior formal or informal understandings with respect to the subject matter hereof.

Exhibit A: Axiad Cloud Service Level Agreement (SLA)

1. Introduction

This Axiad Cloud Service Level Agreement (“SLA”) is a policy governing the use of Axiad Cloud (“Axiad Cloud”) services: “Privileged User”, “Non-Privileged User”, “IoT for Enterprise” and “Trusted Community” under the terms of the Axiad Cloud Service Agreement (the “Axiad Cloud Service Agreement”) between Axiad IDS, Inc. and its affiliates (“Axiad” or “we”) and customers of Axiad Cloud services (“Customer”).

This SLA applies separately to Customer using Axiad Cloud. Unless otherwise provided herein, this SLA is subject to the terms of the Axiad Cloud Service Agreement and capitalized terms will have the meaning specified in the Axiad Cloud Service Agreement. We reserve the right to change the terms of this SLA in accordance with the Axiad Cloud Service Agreement.

2. Definitions

Monthly Uptime Percentage

“Monthly Uptime Percentage” is calculated by subtracting from 100% the percentage of minutes during the month in which Axiad Cloud, as applicable, was in the state of “Critical Service Unavailable” or “Non-Critical Service Unavailable”.

Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Axiad Cloud SLA Exclusion (defined below).

Critical or Non Critical Service Unavailability

“Critical Service Unavailability” and “Non-Critical Service Unavailability” mean that any of the following Services are not available, meaning for each of the following services:

Critical Services Unavailability

- Certificate Revocation Lists Not available or invalid
- Authentication service failing or not responding
- HTTP Rest API authentication failing or not responding

Non-Critical Services Unavailability

- Any other Axiad Cloud API not available
- Any Axiad Cloud portal not available
- PKI Enrollment Services not available

Service Credit



A “Service Credit” is a dollar credit, calculated as set forth below, that we may credit back to an eligible Customer.

3. Service Commitment

Axiad will use commercially reasonable efforts to make Axiad Cloud available with a Monthly Uptime Percentage (defined below), in each case during any monthly cycle (the “Service Commitment”).

Services	Monthly Uptime Guarantee
Critical Services	99.9%
Non-Critical Services	99.5%

In the event Axiad Cloud does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

4. Service Commitments and Service Credits

Service Credits are calculated as a percentage of the total yearly recurring fees paid by Customer (excluding one-time payments such as consulting, professional services etc.) for Axiad Cloud.

Monthly Downtime	Service Credit
Under 99.9% but higher than 99.5% (Applicable only to Critical Services)	10%
Under 99.5% but higher than 99.0%	15%
Under 99.0%	25%

Service Credits will be only applied against future Axiad Cloud payments otherwise due by Customer.

Service Credits will not entitle Customer to any refund or other payment from Axiad IDS.

Unless otherwise provided in the Axiad Cloud Service Agreement, Customer’s sole and exclusive remedy for any unavailability, non-performance, or other failure by Axiad to provide Axiad Cloud is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

5. Credit Request and Payment Procedures

To receive a Service Credit, Customer must submit a claim by opening a case with Axiad Cloud Support (support@axiadids.com)



To be eligible, the credit request must be received by us within 30 days of the Unavailability and must include:

1. Reference to “SLA Credit Request” in the email subject line;
2. The dates and times of each Unavailability incident that you are claiming;
3. The affected Axiad Cloud Services; and
4. Logs that document the errors and corroborate Customer’s claimed outage (any confidential, sensitive or Personal Data (PII) information in these logs must be removed from the logs and replaced with asterisks if applicable).

Note: Logs that contain Personal Data, keys, credentials, or any data deemed as confidential by Axiad will be rejected and immediately deleted.

If the Monthly Uptime Percentage of such request is confirmed by Axiad and is less than the Service Commitment, then Axiad will issue a Service Credit to Customer.

Failure to send the request in due time or to provide required information defined above will disqualify Customer from receiving a Service Credit.

6. Maintenance Window

Axiad IDS uses maintenance windows to bring new features and fixes to your Axiad Cloud instance. Maintenance windows occur weekly and last from 6PM to 12AM Pacific Standard Time.

Our aim is to minimize any downtime during this maintenance window to less than 15 minutes.

In rare cases where a major component of Axiad Cloud is going to be updated, Axiad IDS will provide e-mail notification of such updates 10 business day before the start of the maintenance window.

7. Customer Requirements

Customer is using a highly reliable Internet connection with an average ping response time to AWS US-East datacenter under 250ms.

Customer establishes and maintains a highly available IPSec VPN link to Axiad Cloud VPC.

Customer maintains a reliable internal networking from IPSec gateway to Customer LDAP / Active Directory, and issuance workstation subnets (less 1% packet drop, response time under 250ms when measured from VPC).

Customer maintains a working LDAP / Active Directory service, including working service account.

8. Axiad Cloud SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Axiad Cloud, or any other Axiad Cloud:



1. That result from a suspension described in Section 8 of the Axiad Cloud Services Agreement;
2. Caused by factors outside of our reasonable control, including any force majeure event or Internet access or cloud infrastructure provider outage or related problems beyond the demarcation point of Axiad Cloud;
3. That result from any actions or inactions of Customer or any third party, including failure to acknowledge a connectivity problem outside of Axiad Cloud VPC, and failure to meet the Customer Requirements as defined in previous section (Section 7);
4. That result from Customer's equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within Customer's direct control);
5. That result from down time during planned maintenance windows;
6. That result from any maintenance as provided for pursuant to the Axiad Cloud Service Agreement; or
7. Arising from Axiad's suspension and termination of Customer's right to use Axiad Cloud in accordance with the Axiad Cloud Service Agreement (collectively, the "Axiad Cloud SLA Exclusions").

If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then Axiad may issue a Service Credit considering such factors at Axiad's only discretion.

Exhibit B: Axiad Cloud Information Security

Data Hosting

The Services are performed and delivered from the following locations:

- Amazon Web Service US East Data Centers – North Virginia;

Customer's backup copies may be hosted on the following sites:

- Amazon Web Service US East Data Centers – North Virginia; and
- any other AWS region in the US.

Security Policy

Axiad shall have a documented security policy that is updated regularly and communicated to the appropriate persons. Axiad shall establish and implement security measures, operational procedures and computer system operation procedures consistent with such policy designed to protect information during its use, processing, storage, distribution and destruction.

Customer's information shall be securitized according to industry standard practices for information security such as ISO/IEC 27002-2013. Each of these domains shall be managed by a person in charge identified by Axiad whose duties shall be documented and communicated. The persons identified by Axiad shall be responsible for ensuring that the applicable security and compliance rules are followed in providing the Services for each of the following areas:

- Security policy;
- Organization of information security;
- Human resources security;
- Asset management;
- Cryptography;
- Physical and environmental security;
- Operation security;
- Telecommunications security;
- Acquisition, development and maintenance of information systems;
- Axiad management;
- Management of information security-related incidents;
- Business continuity management.



Information Security

Axiad Security Officer

Axiad shall designate in writing a person in charge of compliance with the security and compliance rules applicable to the Services. Axiad shall also ensure that information security duties are clearly communicated to staff using Customer's information, whether for the protection of particular information or to carry out activities or security procedures. Such person shall also act as the resource person for Customer with respect to security matters. Axiad's designated person as of the Effective Date is:

Jerome Becquart

Email: security_officer@axiad.com

Tel: +1 408 886-0847

Background Checks

Axiad declares that it conducts background checks on its employees with access to sensitive or confidential Customer Data, information and services, which checks report on convictions for fraud, theft and other offenses that could jeopardize the security of sensitive or confidential Customer Data, information and services.

Asset Management

Axiad shall be responsible for maintaining an inventory of its media which contains information of Customer, including computer equipment (e.g., data base servers, storage media, work stations) and paper documents. All such media shall be clearly identified and recorded.

Axiad shall conduct a physical inventory of information media on a regular basis (at least twice a year). Axiad shall also have a procedure allowing discrepancies to be identified and, where applicable, explained. Customer shall be informed of any discrepancy as quickly as possible. Inventory reports shall be submitted to Customer for review, assessment and approval.

Any discrepancy attributable to the loss or theft of equipment shall be treated as a security incident.

Access Control

Axiad shall limit physical and logical access to its systems and sites used in connection with the providing of Services to those of its employees and subcontractors who need access to perform the Services by setting up and implementing an access management procedure and authentication measures in accordance with standard industry practice.

Axiad shall manage access by ensuring the reporting of access, using the need-to-know and least privilege principles and taking appropriate action in a timely manner upon any change to the duties of any of its employees or subcontractors. Mechanisms shall be set up to ensure the separation of incompatible duties. When duties cannot be separated, compensatory controls shall be implemented (e.g., regular review of activity logs).

Physical and Environmental Events

Axiad Cloud is hosted on AWS that is SOC 1, 2 and 3 compliant.



Telecommunications and Exploitation Management

Logging and Monitoring

Axiad shall log security events on the systems used to provide the Services, including activities related to accessing and protecting the logs.

Axiad shall set up and implement procedures for monitoring logs, computer systems, its sites and all pertinent Axiad resources which it operates in connection with Customer's information, in order to detect and report anomalies, including the breach of information security measures, and allow for rapid intervention.

Reported incidents shall be managed according to Axiad Information Security Incident Management Procedure.

Vulnerabilities management

Axiad shall set up and implement a vulnerabilities management procedure which shall include, among other things: procedures to detect and report on vulnerabilities, the diagnosis and treatment of vulnerabilities according to their level of severity, documentation and the communication and follow-up of corrective action. The procedures shall cover the Axiad servers, work stations, telecommunications equipment, operating systems, software platforms (including data bases, source code management systems and web servers) as well as the applications for which the manufacturer's development code is present used by Axiad in providing services.

In the event of vulnerability classified as critical, Axiad shall notify Customer and implement all reasonable measures designed to remedy the breaches and correct the vulnerability as quickly as possible.

Security Patches

Axiad shall keep the Axiad servers, workstations, telecommunication equipment, operating systems, software platforms (including databases) as well as the applications used for which the manufacturers' development code is present up to date, including the security patches in accordance with the recommendations of the relevant manufacturers.

The corrections or new versions shall be tested, approved and deployed in accordance with a change management procedure. Prompt action shall be taken for security patches of urgent/critical severity. High-severity security patches shall be installed within 7 days of being issued in order to reduce the risk of attack unless Customer agrees otherwise. Other patches shall be evaluated, tested and applied during the maintenance window determined for each system.

Malware detection and removal

Axiad shall set up and implement prevention, detection and recovery measures designed to protect against malware. In addition, Axiad shall install software to detect malware on Axiad computer equipment (e.g., servers, computers) used for the collection, use, storage, transmission or destruction of Customer's information. Axiad shall also regularly update the available malware signatures. This procedure shall be communicated upon request to Customer.



Information Transmission

to the extent Axiad is required to transmit Customer information as part of the Services, Axiad shall implement procedures designed to protect all data transmissions to and from external networks (e.g., networks outside the agreed-on architecture, networks of subcontractors, Customer's network or the network of Customer's suppliers, etc.) against interception, copy, modification, re-routing or destruction.

Furthermore, the flow of data to and from external networks along with the envisioned security measures must be documented and approved by Customer prior to implementation.

Vulnerability and Intrusion Tests

All externally facing IP addresses including the production, development and test environments shall be scanned daily with a vulnerability management tool by Axiad.

"Candidate build" images shall also be scanned weekly as part of QA qualification.

All applications interfaces are tested for vulnerabilities quarterly, either by Axiad or by the upstream technology providers.

Unless discovered or reported vulnerabilities require a more urgent schedule, all Axiad environments are patched on a rolling 7-day cycle planned with customers.

Penetration testing by a third party is performed internally and externally every year on the Axiad environment, or after significant changes to the technical environment.

Breaches

Axiad shall notify Customer of any data-security breaches of which Axiad becomes aware that involve Customer information. Axiad shall promptly investigate any such breach and use all reasonable efforts to mitigate the effects of such a breach and to implement measures to prevent such breaches from occurring in the future.

Audit Rights

Customer may conduct an audit of Axiad's facilities to ensure that the Services are rendered in accordance with the terms hereof, including with respect to confidentiality, availability, integrity and security involving confidential information of Customer, and to enable Customer to determine if the Services enable Customer to comply with its regulatory requirements. Customer may conduct any such audit no more than once a year and upon at least fifteen (15) business days' notice. The conduct of such audit shall not materially interfere with Axiad's operations. During such audit, Customer shall not access or be granted access to information of any other Axiad customer, or to any information, system or facilities not used in the performance of the Services.