# STANDARD GLOBAL SUPPORT & MAINTENANCE POLICY

**INTRODUCTION**

Blockchain Security Services and its affiliates Blockchain Security Consulting and Blockchain Development Consulting (collectively, the Company, we or us) will provide our customers (customer, you or your) with support and maintenance services (Support) as described in this Standard Global Support and Maintenance Policy (Policy).

We may update or revise this policy from time to time and will use commercially reasonable efforts to limit material revisions to once annually.

**ELIGIBILITY**

You must pay all applicable fees and have one of the following to qualify for Support under this Policy:

• Current maintenance and support plan for a premise licensed Product;

• Current subscription license for a Product; or

• Current subscription for a cloud, hosted or SaaS Product. “Product” as used in this Policy refers to a Blockchain Security Services software, subscription service or hardware or equipment covered under warranty or a Support plan.

**OBTAINING SUPPORT**

You must be a registered user and have the following information available when contacting us for Support (failure to have this information may delay Support):

• Your company contact information and the caller’s contact information • Problem description • Problem details

• Business impact

• Problem severity

• Exact error messages

• Log information

• Date and time problem was encountered

• Changes made to the configuration/environment prior to the problem

• Changes made to the configuration/environment after the problem

• Actions taken to isolate and resolve before contacting us

• Hardware configuration type

• Appliance version release level (for IdP Products)

• System configuration parameters

• Information about other products and systems interacting with the Product

You can open a support ticket using our Support Portal at https://support.BlockchainSecurity.Services or https://support.coresecurity.com (collectively, the Support Portal).

All Severity Level 1 matters must be reported via phone.

For the best routing, logging a ticket through the Support Portal is preferred for Severity Levels 2 – 4.

You can always follow up by phone to get an update on your ticket.

**Prior to Opening a Support Ticket**

Prior to requesting Support, you must use commercially reasonable efforts to comply with our published operating and troubleshooting procedures. You should also review these helpful tips:

• Search the online help and self-service Knowledge Base solutions by reviewing relevant documents on the Support Portal at https://docs.BlockchainSecurity.Services/

• See if the problem is reproducible.

• Check to see if the problem is isolated to one machine or more.

• Note any recent changes to your systems and environment.

• Note the version of your software and environment details, such as operating system, database, etc.

**Case Registry Contacts**

You must appoint one (1) or more individuals within your organization who are reasonably knowledgeable in the operation of the Product to serve as primary contact between you and the Company regarding the registry and report of Support tickets (the Case Registry Contacts).

All of your Support inquiries should be initialized through your Case Registry Contact(s) when possible. As a security precaution, our Support hotline analyst may request further information to verify the identity of the caller. If at any point, our Support hotline analyst believes that the requesting party is not authorized, as a security precaution, we may deny the Support request until a Case Registry Contact is reached.

Additionally, any request for improper assistance will be reported to your Case Registry Contact(s). Support Ticket Management Process We assign a unique Support request number (Support ID) to all Support tickets. These Support IDs allow us to prioritize and track all Support tickets through to resolution and allow you to get a status update on your case via our Portal.

All Support tickets are assigned a Severity Level and are placed in a queue to be processed by the next available Support Engineer. Support Engineers take ownership of your Support ticket and see it through to successful resolution. The Support Engineer will contact you, gather any additional information needed, and investigate to determine the proper course of action. This may require the Support Engineer to re-create the issue, work with our development team, and/or help you with configuration of the Product.

An administrator from your company is required to have access to the application administrative interface, command line interface and base operating system. Your administrator must have the ability to request additional resources from your company as needed to assist with troubleshooting the environment or application. If our Support Engineer and development team determine that the issue is a product defect, please see the “Product Defects” section in this policy for specific request handling information.

**Escalation Guidelines**

Our goal is to resolve all Support tickets in a satisfactory and timely manner; however, we realize that some situations may require increased attention and focus within our team. You can raise the severity of a Support ticket through the Support Portal or call us and request to speak with a Support Manager. Upon your request, the Support Manager will evaluate the case and create an action plan. If you are not satisfied with the plan or with the progress of the case after the plan has been implemented, you can contact our Technical Support Manager, who will review the Support ticket and determine if different or additional actions are required.

Closing a Support Ticket Support tickets remain open until the issue has been resolved or addressed. Exceptions apply to requests for product enhancements, product defects and where the customer fails to respond to request for information for 5 business days or longer. You also can close requests via our Portal.

Re-Opening a Support Request You can re-open your closed Support ticket from the Portal.

**SEVERITY LEVELS AND RESPONSE TIMES**

All Support tickets are assigned a severity level from 1 to 4 based on the technical and business impact of the reported problem. As troubleshooting progresses, we will work with you to reassess the technical and business impact of the problem and, if appropriate, adjust the case severity level.

**SECURITY LEVELS**

- Basic Support is available for purchase with premise perpetual licenses and is included with all subscription licenses and cloud (SaaS) subscriptions.
- Premier Support and Mission Critical Support are available for an additional cost for certain Products.

**PRODUCT UPDATES**

In accordance with this Policy, you have access to all updates, version releases, upgrades, and enhancements to the Products that are not designated by us as new products or modules for which we charge a separate fee. If you are eligible for Support and have a current perpetual license, subscription license or subscription access for the Product then you may install and use all Product upgrades, updates and enhancements and we strongly encourage you to do so, provided, however, that you may be required to install the current or future version in order to resolve your Support issue. Failure to install the upgrades, updates and enhancements may result in ineligibility to receive Support under this Policy. If you have a current subscription for a cloud or SaaS Product then we will be responsible for upgrading, updating and enhancing the cloud platform. Any corrections to the Product will be made to the current generally available release of the Product.

**HARDWARE & EQUIPMENT SUPPORT**

Only hardware that has been provided by and warranted by the Company is eligible for Support. Computer equipment and appliances obtained, licensed or purchased by you (either directly or through us) from third party vendors are not eligible for Support. For hardware covered under warranty, you may return non-working hardware after obtaining a Return Materials Authorization (RMA) number from us. The issuance of an RMA is not an admission that the hardware is defective. We will repair or replace defective hardware, at our discretion. You are responsible for all costs of shipping and insurance for the return of the hardware to us, and we will pay all costs of shipping and insurance for the return of the hardware to you. You agree that we may perform remote testing on hardware, where applicable, prior to the issuance of an RMA number. If you have customized hardware appliances from us, then the annual fee for continuously upgrading the customized hardware appliances to the latest software release is twenty percent (20%) of the original development cost of each customized hardware appliance. Hardware not under a warranty or current support plan is not eligible for Support under this Policy. Additional charges will apply if we agree (at our sole discretion) to repair or replace such hardware.

**COMPANY RESPONSIBILITIES**

We have employees in offices worldwide to provide Support. We use follow-the-sun practices to provide 24 x 7 x 365 Support for Severity 1.

We will provide Support for Severity 2, 3 and 4 issues and for all other products from 7:00 AM to 7:00 PM EST, Monday through Friday, excluding our recognized holidays.

We will:

a. Deliver Support in English (we may offer limited assistance in languages other than English based on resource availability).

b. Deliver Support by our staff or other qualified and authorized partner personnel.

c. Use reasonable efforts to determine if a Product problem exists based on the information you provide, and the information generally known to us.

d. Investigate and remediate known problems for the Products as available.

e. Provide technical assistance and troubleshooting to resolve problems or defects when the covered Product does not function substantially as described in the published technical specifications.

f. Remotely troubleshoot issues to determine the cause of a technical problem relating to the functionality or disruption of the Product.

g. Provide problem management and reporting using our Support case tracking system.

h. Use best efforts to respond to reported problems within the targeted time frames and provide status updates during the resolution process.

i. Resolve defects on supported Product releases and provide Product updates, which may contain code fixes, improvements or enhancements to existing functionality.

j. Defect fixes can be delivered as an immediate code fix or as part of a future Product update or upgrade release at our discretion.

k. Ensure that third-party software embedded in a Product functions with the Product as described in the applicable technical specifications and make commercially reasonable efforts to maintain the embedded third-party software at a version supported by the vendor. As a general practice, third-party software patches and upgrades will be tested and included with Product upgrades.

l. Provide Support for Product releases until the published End of Life (EOL) date.

m. Interface with vendors to provide support for vendor supported products.

n. Subject to your responsibility for data protection in accordance with this Policy and any provisions of the agreement between you and the Company or any separate agreement on data protection, we will maintain administrative, physical, and technical safeguards to ensure the security, confidentiality and integrity of data we may process as a result of providing you Support.

We will:

• limit our collection and storage of your data to the minimal amount necessary to provide Support for an incident;

• store collected data in secure encrypted locations; • limit access to authorized employees based on their job function;

• ensure all authorized employees complete security training;

• maintain Company employee access rights using our HR provided employee status data;

• ensure access to all data storage locations complies with our password maintenance and update policies; and

• maintain card key access to all Company managed data storage locations and Support offices. YOUR

**RIGHTS AND OBLIGATIONS**

You must:

a. Provide accurate and complete contact information at all times to enable us to send email or other notifications from time to time, and such other information as is required by us under this Policy to enable us to respond to your requests for Support.

b. Before production use of the Product, provide us with an operational architecture document which describes how the Product is being used in your environment. Documents created as part of your internal support processes and which provide all relevant information needed for us to help troubleshoot problems are acceptable substitutes.

c. Maintain currency with supported versions of the Product releases.

d. Select, purchase, configure, operate and maintain your equipment, hardware, facilities, network and Internet, data and telephone connections necessary for use and support of the Product.

e. Maintain proper Product environment in accordance with Product technical specifications or as may be reasonably expected in accordance with industry standards.

f. Maintain a current backup copy of the Product and all of your data and keep backup copies in a safe location reasonably accessible to Company personnel if we require access to maintain the Products.

g. Payment of any additional third party licensing fees associated with third-party software as part of Product updates and upgrades.

h. Provide us with reasonably necessary access to your personnel and equipment required to resolve the Support issue; including, if required by us, remote access to your systems as necessary to enable us to perform Support.

i. Provide supervision, control and management of the use of the Product.

j. Implement procedures for the protection of information and the implementation of backup facilities in the event of errors or malfunction of the Product or related equipment.

k. Maintain a current backup copy of all of your programs and data.

l. Take all steps reasonably necessary to carry out procedures for the rectification of errors or malfunctions within a reasonable time after you receive the procedures from us.

m. Properly train your personnel in the use and application of the Product.

n. Report all detected errors or malfunctions of the Product to us.

o. Request Support as outlined in this Policy.

p. Cooperate with us to enable the troubleshooting of reported incidents.

q. Use the Product in accordance with the Product documentation.

**Customer Data**

You are aware that access to login data, employee contact information, application log files, or data files may be required by us in order to provide Support. Such files may contain personal data, including, but not limited to, names of individuals, email addresses or other personal data. You are solely responsible for complying with any data protection laws, including using principles of data avoidance and data minimization, by taking measures to mask, strip or anonymize personal data when providing us access to original or copies of data files. You will use reasonable efforts to prevent disclosure to us of any personal information. We, our affiliates, licensors and agents are not responsible for compliance with such laws and do not assume any liability with respect to any infringements of any laws in relation to the use of our Support services by you.

The provisions of the license or subscription agreement between you and the Company or any separate agreement on data protection remains unaffected.

**Data Sharing**

Customer understands that certain Products collect various data including, but not limited to, DNS or network traffic patterns and other data or information relating to malicious or potentially malicious

activity within the customer network environment (Data Sharing) as further detailed in the applicable Product documentation. You acknowledge and agree to participate in Data Sharing. You may notify us in writing if at any time you elect to either commence or discontinue Data Sharing and you agree to pay the associated fees for not participating in Data Sharing. You expressly agree that we may use all Data Sharing information and any derivative thereof in order to analyze, assess and respond to malware and other threats, including in the course of providing services to other customers; provided, however, that we will not disclose any Data Sharing information to other customers. You represent, warrant and covenant that your participation in Data Sharing does not violate any law or regulation and that you have provided any required notices to and/or obtained any required consents from your end-users for the collection, use and processing of information provided to us pursuant to the Data Sharing arrangement.

**SUPPORT EXCLUSIONS**

The following items are not included in Support. If you request assistance for, or as a result of, any of these items, we may offer to provide assistance at our then current time and materials rates by issuing a quotation or statement of work. Further, if the occurrence or existence of any of the following causes us to be unable to fulfill our Support obligations to you, we will not be responsible for meeting those obligations.

a. Services related to hardware or software installation.

b. Additions, configuration, or activations of new features or functionality of the covered Product.

c. Consulting or on-site services.

d. Training or usage assistance.

e. Project management.

f. Support for your network or environment.

g. Guaranteed bug fixes for all problems.

h. Product programs made by you or other parties under your control or direction.

i. Problems resulting from any service or product not provided by us (we are not responsible for the maintenance, administration or support (including procurement and installation of updates, patches, defect fixes, and upgrades) of your operating system software, hardware and software).

j. Problems resulting from customer’s modification, customization, alteration or addition or attempted modification, customization, alteration or addition to the Product undertaken by any party other than us or our agents without our written consent.

k. Problems resulting from customer’s negligence, error or misuse of the Product.

l. Problems with customer’s hardware, software, network infrastructure and services, or Internet access.

m. Problems resulting from inadequate or improperly configured servers, networks, storage, and other underlying infrastructure supporting the execution of the Product.

n. Problems arising from customer's failure to properly use or install the Products in accordance with applicable Product documentation or customer's license or subscription agreement with us.

o. Problems caused by Product or telecommunication interfaces not meeting or not maintained in accordance with the manufacturer's specifications.

p. Problems that have been addressed in a software update that customer has elected not to apply.

q. Problems caused by customer's failure to maintain all software at the same software update and upgrade levels.

r. Problems caused by customer's data.

s. Changes to, resolution of, or support for resolution of incidents or errors caused by network, desktop, host configurations, hardware or software other than the Product.

t. Support limitations (e.g., standard, limited, extended, EOL) as described in this Policy in the "Product Update" section above.

u. Third party services; including procurement and installation of any third-party software or hardware required to be provided by the customer for the implementation of Product or upgrades.

v. Support for third-party operating system software, third-party software, hardware, or firmware not procured from us.

w. Problems resulting from relocation or the addition of accessories, attachments or other devices to hardware procured and warranted by us.

x. Any customer or third-party infrastructure components, including but not limited to:

• Blockchains

• Identity Stores, including but not limited to: Microsoft Active Directory, Microsoft Active Directory Lightweight Directory Services (LDS), OpenLDAP, Novell e-Directory, IBM LDAP, Sun One LSAP, ApacheDS, any other third-party Lightweight Directory Access Protocol (LDAP) directories, Microsoft SQL Server, Oracle Server, Google Apps Datastore, and any other identity or profile store;

• Third-party Databases, Datastores, or SIEM products (whether on-premise or cloud hosted) used for the storage and reporting of any audit, accounting, or reporting data;

• Underlying hypervisors or hypervisor management products used to host and support a Virtual Appliance, including but not limited to: Microsoft Hyper-V, VMware ESx, and Citrix XenServer;

• Mobile device management (MDM) solutions used to manage any endpoints or mobile devices; 4

• Support of endpoint Operating Systems (including, but not limited to: Microsoft Windows, Apple OS X, Mac OS, Linux and Unix Derivatives) and Mobile Operating Systems (including, but not limited to: Apple iOS, Android, Windows Mobile/Phone, and Blackberry);

• Underlying private or public network infrastructure - both physical and logical;

• Cloud or third-party hosting services not provided by us;

• Third-party hardware OTP tokens, proximity cards, smart cards and reader devices; and

• Relying party product, such as those that accept SAML or other assertions from the Product.

y. Proof of concept, free trial or evaluation Product environments.

z. Support of the Product for purposes other than the purposes for which the Product was designed. aa. Customer's failure to perform its obligations under this Policy. bb. Other problems not within our control (including internet service failures or delays; unusual physical, electrical or electromagnetic stress; failure or fluctuation of electric power, air conditioning or humidity control; excessive heating; fire and smoke damage; failure of backup/rotation media not furnished by us).

**END OF AVAILABILITY**

We may, at our discretion, decide to retire a Product from time to time (End of Life or EOL). We will publicly post for all customers notice of EOL, including the last date of general commercial availability of the affected Product and the timeline for discontinuing Support. We will have no obligation to provide Support for a Product that is outside of the applicable EOL period. [Revised September 2018].