CLOUD SERVICES ADDITIONAL TERMS

Service Schedule 2

This Service Schedule 2 – Cloud Services Additional Terms applies to the Cloud Services provided by Skyhigh Security (respectively) (the "Company," "We," "Us," "Our") based on the SKU purchased by the Customer ("You" or "Your"). All capitalized terms not defined herein shall have the meaning provided in your underlying cloud services agreement.

1. **Support and Customer Plans for Skyhigh Security:** We will provide Support to You in accordance with the applicable Skyhigh Security Service Schedule located in the Exhibit 1 - SKYHIGH SECURITY SUPPORT & CUSTOMER PLANS.

2. **Definitions:**

Business Day means any day other than a Saturday, Sunday, statutory or public holiday in the place where Company Products are provided, or the Professional Services are performed.

Cloud Services means the Cloud Services that We provide to You as specified in one or more Grant Letters and that are subject to the applicable Service Schedule.

Company means:

i. **Musarubra US LLC**, located at 2611 Internet Blvd., Suite 200, Frisco, TX 75034 USA, if the Cloud Services are purchased in the United States (except as provided in Subsection (vii) below), Canada, Mexico, Central America, South America, or the Caribbean;

ii. **Musarubra Australia Pty Ltd**., located at 40 Mount Street, Level 16, North Sydney, NSW 2060, Australia, if the Cloud Services are purchased in Australia.

iii. **Musarubra Ireland Limited**, located at Building 2000, City Gate, Mahon, Cork, Ireland, if the Cloud Services are purchased in Europe, the Middle East or Africa;

iv. **Musarubra Japan KK**, located at Shibuya Mark City West, 1-12- 1 Dogenzaka, Shibuya-ku, Tokyo 150-0043, Japan, with respect to the distribution of the Software, and the provision of all Cloud Services and Support, purchased in Japan;

v. **Musarubra Singapore Pte Ltd**., located at 38 Beach Road, #23-11, South Beach Tower Singapore, 189767, with a copy to legal@trellix.com and with respect to the distribution of Software license purchased in Asia Pacific (but excluding China (RMB) or Austraila), and provision of all Cloud Services and Support purchased in Asia Pacific (but excluding China (in RMB) or Australia);

vi. **Trellix (Beijing) Security Software Co., Ltd**., located at Room 608, Unit 610, 6/F Zhongyu Masion, No.6 North Workers' Stadium Road, Chaoyang District, Beijing, China, if the Cloud Services are purchased in China (in RMB); or

vii. **Trellix Public Sector LLC**, located at 1640 Boro Place, 3rd Floor, McLean, Virginia 22102, USA, if the Cloud Services are purchased by the U.S. Government, state or local governments, healthcare organization or educational institutions within the United States.

Customer means the entity which has purchased Products and to which We provide Support.

Grant Letter means any written (electronic or otherwise) confirmation notice that We issue to You confirming the Products purchased and applicable Product Entitlement. The Grant Letter identifies the SKU number, quantity, Subscription Period or Support Period, and any other access and use details.

Product Entitlement means the license or subscription types set forth in the Grant Letter and defined at https://www.skyhighsecurity.com/wp-content/themes/skyhigh-security/public/SkyhighSecurity_Product_Entitlement_Definitions_7_27.pdf

Data means Your Personal Data, sensitive data or other information about You and Users (including Users' name, address, e-mail address and payment details), their computers, files stored on their computers, or their computers' interactions with other computers (including information regarding network, licenses used, hardware type, model, hard disk size, CPU type, disk type, RAM size, 32 or 64 bit architecture, operating system types, versions, locale, BIOS version, BIOS model, total scanners deployed, database size, system telemetry, device ID, IP address, location, content, products installed, components, processes and services information, frequency and details of update of Our components, information about third-party products installed, extracts of logs created by Us, usage patterns of Our products and specific features, etc.

SKUs means A Stock Keeping Unit is a unique identifier for each distinct product and service that can be ordered from Us.

Subscription Period means the period for which You have purchased the right to receive the Cloud Services or the time-period for which You have purchased the right to receive Support, as applicable.

Support means the technical support services that We provide for the support and maintenance of the Cloud Services, as specified in the applicable Service Schedule.

Support Period means the period for which You are entitled to Support, as specified in a Grant Letter.

User means a unique individual whom You have authorized to use the Cloud Services pursuant to Your access rights under this Agreement, including Your employees, Your Affiliates, subcontractors, authorized agents, and Managed Parties.

EXHIBIT 1

SKYHIGH SECURITY SUPPORT & CUSTOMER PLANS

We will provide Support for the Cloud Services in accordance with the following:

Support and Maintenance	
Support Requests	
Phone	1-866-727-8383
Skyhigh Security Web Link	https://www.skyhighsecurity.com/support.html
Phone & Web	24x7x365 or 8x5 within business hours (depending on Service Level)
Technical Support	
Office hours (critical and non-critical issues)	24x7x365 or 8x5 within business hours (depending on Service Level)
Availability for critical issues	24x7x365 or 8x5 within business hours (depending on Service Level)
Response time	See below
Service Support	
Upgrade notifications	Yes, SNS notification will be provided
Remote diagnostics	Yes, we have the capability to connect to your network
Online Resources	
Documentation	https://success.myshn.net/

The Parties will jointly use the severity levels below to document and respond to errors or deficiencies that may exist. If You believe that an error or deficiency exists in the programs supported by the subscription fees under this Agreement, You will provide written notification to Us of such error or deficiency, along with supporting data and programs that document such error or deficiency. We will respond in accordance with the following severity levels.

Severity Levels

Critical - Severity 1 Error:

A "*Severity 1 Error*" will mean that the Cloud Services is non-operational, and no Users can access the system, or the functionality is significantly decreased, or back-up or other security of data can no longer be performed. The defect affects mission-critical systems or information in the production environment. This may include any defect related to You or personal safety, system availability, overall data integrity or ability to serve You.

"Severity 1 Error" events will require immediate resolution. We must start the correction of "Severity 1 Errors no later than thirty (30) minutes following notification from You. We will work to correct Severity 1 Errors on a 24x7 basis until resolution. Our Support personnel as well as Your personnel may be required to sustain a twenty-four (24) hour per day effort to determine the root cause of the problem or until circumvention or resolution is provided. We will provide regular updates informing You of the progress to remedy the reported problem. For Severity 1 Errors only, telephone support is available to report irregularities twenty-four (24) hours per day seven (7) days per week.

High - Severity 2 Error:

A "*Severity 2 Error*" will mean that the Cloud Services is operational with functional limitations or restrictions but there is minimal business impact. The error has a large impact on the functionality of the application but does not require immediate release into the production environment.

We must start the correction of "Severity 2 Error" no later than one (1) hour following notification by You. We will work to correct Severity 2 Errors during normal business hours and will provide regular updates informing You of the progress to remedy the reported problem.

Medium - Severity 3 Error:

A "*Severity 3 Error*" will mean these Cloud Service is operational with functional limitations or restrictions that are not critical to the overall system operation. The error has a moderate impact on the functionality of the application. However, the Service remains usable by all groups.

We will work to correct Severity 3 Errors during normal business hours. We will use reasonable efforts to correct such errors within thirty (30) business days.

Low - Severity 4 Error:

A "*Severity 4 Error*" will mean the Cloud Service is operational with problems or errors, which have little impact on system operations. Severity 4 Errors will include documentation errors. The error has a minor impact on the functionality of the application.

"Severity 4 Error" events are normally corrected in the next maintenance release of the Cloud Service.

To Contact Us, please reach out to Your Customer Support Manager or through the Skyhigh Support Service Portal at https://www.skyhighsecurity.com/support.html

Services	No Service Level	Foundation	Advanced	Premier	Pinnacle
Support Hours	8x5 Business Hours	24x7x365	24x7x365	24x7x365	24x7x365
Support Initial Response Target	Within business hours only Sev 1: 2 Hours Sev 2: 4 Hours Sev 3: Next Business Day Sev 4: Next Business Day	Sev 1: 2 Hours Sev 2: 4 Hours Sev 3: 8 hours Sev 4: Next Business Day	Sev 1: 2 Hours Sev 2: 4 Hours Sev 3: 8 hours Sev 4: Next Business Day	Sev 1: 1 Hours Sev 2: 2 Hours Sev 3: 4 Hours Sev 4: 8 Hours	Sev 1: 1 Hours Sev 2: 2 Hours Sev 3: 4 Hours Sev 4: 8 Hours
Support Request Source	Web Portal and Phone	Web Portal and Phone	Web Portal and Phone	Web Portal and Phone	Web Portal and Phone
Knowledge Base & Documentation Access	Yes	Yes	Yes	Yes	Yes
Ticket Routing	Standard Pool	Standard Pool	Standard Pool	High Touch Pool	High Touch Pool
Language Support (Non-English Best Efforts)	English Only	English, German, Korean, Japanese	English, German, Korean, Japanese	English, German, Korean, Japanese	English, German, Korean, Japanese
Incident Management	Yes (RCA for Sev 1 incidents upon request only)	Yes (RCA for Sev 1 incidents only)	Yes (RCA for Sev 1 incidents only)	Yes (RCA for Sev 1 incidents and select Sev 2 incidents; On-demand Q&A, RCA walkthrough)	Yes (RCA for Sev 1 incidents and select Sev 2 incidents; On-demand Q&A, RCA walkthrough)
Update / Maintenance / Incident Notification	Skyhigh Status Page	Skyhigh Status Page	Skyhigh Status Page Direct Messaging (Email)	Skyhigh Status Page Direct Messaging (Email)	Skyhigh Status Page Direct Messaging (Email)

Services	No Service Level	Foundation	Advanced	Premier	Pinnacle
Technical Consulting Services [1]					
Additional feature configurations (per year) [1]	-	-	1	2	Unlimited
Software Upgrade Assistance [1]	-	-	Yes	Yes	Unlimited
Limited Availability Feature Access [1]	-	-	Yes	Yes	Yes
Adoption & Value Realization Services [1]					
Success Planning (Mutual Value Plan)	-	-	Managed	Managed	Managed
Health watch vouchers (per year) [1]	-	1	1	2	4
Configuration review vouchers (per year) [1]	-	-	1	2	4
Training & Enablement [1]					
Access to free eLearning modules [1]	Yes	Yes	Yes	Yes	Yes
Instructor-led training (attendees per year) [1]	-	-	2 pax	4 pax	6 pax
Governance & Advisory					
Operational service review	-	-	Fortnightly	Weekly	Weekly
Business review	-	-	Semi-annually	Quarterly	Quarterly
Product Partnership					
Product Roadmap Visibility	-	-	-	Yes	Yes
Early Access Program	-	-	-	Yes	Yes
Design Partners Forum	-	-	Yes	Yes	Yes
Customer Advisory Board	-	-	Yes	Yes	Yes

[1]Appendix 1

Technical Consulting Services

- Feature configuration must be selected from a list of available features[2] and will be limited to the existing deployed solution
- Upgrade assistance will be limited to software updates only; Software upgrades will be guided by documentation and a Skyhigh Security expert will oversee and assist the customer team as needed; for hardware upgrades and installation, please consult with your account manager for options
- Limited availability features will be made accessible with guided support

Services	No Service Level	Foundation	Advanced	Premier	Pinnacle
Technical Consulting Services					
Additional feature configurations (per year) (see Appendix)	-	-	1	2	Unlimited
Software Upgrade Assistance	-	-	Up to 2 on-prem device clusters (max 10 devices) OR Up to 1 cloud connector upgrade	Up to 4 on-prem device clusters (max 20 devices) OR Up to 2 cloud connector upgrades	Unlimited
Limited Availability Feature Access	-	-	Yes	Yes	Yes

Adoption & Value Realization Services

- **Health watch and configuration review**
  - A health watch or configuration review will cover one deployed solution (out of SWG on-prem, SWG cloud, CASB, or Private Access).
  - The scope and deliverables will be defined at the start of the exercise.
- **Training & Enablement**
  - Access to free eLearning modules (for unlimited users): Access is available to any number of Skyhigh Security dashboard users, but limited to the following modules:
    - Secure Web Gateway Fundamentals for Cloud
    - Secure Web Gateway Fundamentals for On-premises Appliances
    - Skyhigh Security Cloud Fundamentals

Services	No Service Level	Foundation	Advanced	Premier	Pinnacle
Adoption & Value Realization Services					
Health watch vouchers (per year)	-	1 (Up to 2 clusters for SWG on-prem)	1 (Up to 4 clusters for SWG on-prem)	2 (Up to 6 clusters for SWG on-prem)	4 (Up to 10 clusters for SWG on-prem)
Configuration review vouchers (per year)	-	-	1 (Up to 4 clusters for SWG on-prem)	2 (Up to 6 clusters for SWG on-prem)	4 (Up to 10 clusters for SWG on-prem)

  - Instructor-led training:
    - A specified number of attendees per year can attend a standard instructor-led training courses with hands-on labs in a shared classroom.
    - A dedicated classroom requires minimum 6 attendees.

- Custom trainings are not included in this entitlement. They must be scoped separately and may incur additional costs.
- Additional training seats can be allocated against purchase of training vouchers.

[2] Appendix 2

Additional Feature Configurations

Definitions

- Feature: A "feature" is defined as a single capability/function of the product that can be enabled and configured independently to deliver specific business value.
- Baseline Features: Must-have features required for successful product deployment. These are included in the initial deployment or rollout and are not in scope as part of the Service Levels.
- Eligible Features: Supported by the product but not deployed during initial deployment. Eligible Features are divided into two categories:
  - Recommended Features – Provide significant security and operational value; strongly advised for most customers.
  - Advanced Features – Extended capabilities designed for organizations with mature use cases or specialized needs.
- Exclusions
  - Baseline features already deployed as part of initial implementation.
  - Any custom development, integrations, or features not included in the official product catalogue.
  - Development of custom scripts, automation, or integrations with third-party products unless explicitly stated.
  - Activities outside the scope of deployment and enablement (e.g., ongoing operations, managed services).
- Customer Obligations
  - To ensure successful enablement, the customer will:
  - Provide required system access, admin credentials, and test environments
  - Ensure licenses and subscriptions for selected features are active.
  - Complete prerequisite infrastructure or configuration steps (as advised).
  - Assign appropriate stakeholders for requirements gathering, testing, and validation.
  - Participate in knowledge transfer and handover sessions.
  - Customers are encouraged to provide advance coordination when requesting feature enablement to allow for resource scheduling and preparation.
- Validity & Consumption
  - Customers are entitled to enable any Eligible Features within 1 year from subscription start date.
  - Feature enablement does not need to be finalized during project kickoff; selections can be made anytime within the validity period.
  - Unused entitlements will expire after the 1-year window and cannot be carried over.
  - Each feature enablement is considered consumed once deployment activities are initiated.
- Change Management
  - Requests to add, modify, or replace features outside the predefined Eligible Feature catalogue will be treated as Change Requests and may require a separate scoping and approval.
  - Any scope adjustments must be mutually agreed upon in writing prior to execution.
- Knowledge Transfer
  - For every feature enabled, the Skyhigh Security team will conduct a Knowledge Transfer (KT) session with the customer team.
  - KT will include deployment overview, configuration details, and operational best practices.
  - Documentation and guidance will be shared where applicable to support customer self-sufficiency.

Examples of Eligible Features

Secure Web Gateway

- Custom Block/Coaching Pages
- Integration with Sandbox Solutions (IVX)
- Media Type Filtering Configuration
- Gateway Antimalware Setup
- Web Data Loss Prevention (DLP)
- Content Security Reporting (CSR)
- Shadow IT Integration + Closed Loop Remediation (CLR)
- Dynamic Content Classification
- High Availability Setup
- Cluster Manager Setup
- Log Export & Forwarding
- Integration with Remote browser Isolation
- Web Hybrid Setup
- Advanced Web Traffic & Connection Control
- Appliance Performance & Event Monitoring (with SNMP Integration)
- YouTube Access Control
- Fallback Authentication Setup
- Application Filtering Configuration
- Advanced User Administration Settings
- Bandwidth Control & Management
- REST API Interface
- Microsoft Entra Integration (User Group Lookup)
- Integration with Hardware Security Modules (HSM)
- HTML Content Filtering

Secure Web Gateway Cloud

- Custom Block/Coaching Pages
- Media Type Filtering Configuration
- YouTube Access Control
- Web Data Loss Prevention (DLP)
- SAML SSO Integration
- SIEM Integration (Inline) - Log Collector
- SIEM Integration (Inline) - Log Stream
- Advanced Web Traffic & Connection Control
- Advanced Application Control use cases
- ChatGPT and AI apps Controls
- SAML Authentication
- Integration with Sandbox Solutions (IVX)
- REST API Interface
- Microsoft Entra Integration (User Group Lookup)
- Skyhigh Security Dedicated Egress IP
- Configure Custom Reports & Notifications
- Device Posture Configuration and usage
- Browser Controls
- ICAP Integration
- Risky Web
- Full Isolation

Private Access

- Connector Stickiness
- Configure Device Posture
- Clientless Access
- Access Private Applications from Mobile Devices
- SAML Authentication
- Integration with Trellix EPO (On-prem/SaaS)
- Source IP Anchoring Using Skyhigh Security Private Access

Firewall as a Service

- Configure Device Profiles

CASB: SaaS

- SAML SSO Integration
- Active Directory Integration for user groups
- SIEM Integration
- Enablement of Fingerprint use cases
- Enablement of Malware Inspection Policies
- Enablement of Connected Apps Policies
- On Demand Scans
- Azure Data Storage Enablement
- AWS Data Storage Enablement
- Custom Email Templates & Notifications & Reports
- Anomaly Settings (Whitelisting Allowed Network/Location)
- Enablement of OCR Feature

- SaaS Security Posture Management (SSPM)
- AI & ML Auto Classifier, False Positives
- End User Remediation
- Data Jurisdiction Enablement
- IP Allow List
- SMTP Integration
- DRM Integration (Seclore, Ionic)
- Data Classification Integration (AIP)
- Enterprise DLP Integration
- Anomaly Exceptions
- Finetune DLP Policies (up to 5 Policies)
- Finetune Cloud Access Policies (Up to 5 Policies)

CASB: IaaS

- On-Demand DLP Scan for Storage Services
- On-Demand Malware Scan for Storage Services
- Enablement of Shift Left (Monitor mode)
- NRT DLP for Storage Services
- NRT Malware Inspection for Storage Services
- Enablement of Shift Left (Inline mode)
- Custom Configuration Audit Policy Creation (Up to 5 Policies)
- Custom Email Templates & Notifications & Reports
- Onboard additional IaaS accounts

CASB: Shadow IT

- SAML SSO Integration
- Active Directory Integration for user enrichment
- SIEM Integration
- Service Groups (Governance Rules)
- Closed Loop Remediation (CLR)
- Enablement of Tokenization
- Additional Log Source Setup
- Data Jurisdiction Enablement
- IP Allow List
- SMTP Integration
- IP-Username Mapping
- Configure Custom Reports & Notifications
- Tagging Configuration based on log data location

-End of Service Schedule-