Service Description PaySafe Unified Threat Management Service

The terms and conditions set forth in this Service Description are applicable to PaySafe Unified Threat Management ("UTM") Service purchased through PDI Technologies, Inc. ("PDI") or any PDI affiliate and are incorporated, by reference, into the Agreement between PDI and Customer. Additional information regarding the services, contract term, fees, etc. will be specified in your Agreement and Order Form.

1. **Service Overview**

Unified Threat Management (UTM) refers to a category of network appliances that utilize multiple security features in a single device. Typical UTM applications can include or combine a traditional firewall with VPN, content filtering, anti-virus, anti-malware, intrusion detection (IDS) and intrusion prevention (IPS) capabilities.

PDI's PaySafe UTM service provides a comprehensive, layered security approach to sensitive environments. The PaySafe UTM allows PDI to monitor, with multiple applications, the Customer environment, providing a "single pane of glass" view for more efficient security responses.

PDI's ongoing monitoring and management of appliances deployed on the edge of sensitive environments is reinforced with proactive, bi-annual audits of firewall configurations. As security best practices mature, UTM services and configurations are dynamically updated as well.

2. **Service Activation**

PDI's activation of its PaySafe UTM Service (the "Service Activation") consists of the three main phases: Discovery & Onboarding; Deployment; and Validation.

2.1. Discovery & Onboarding

During the onboarding process, Customer will submit to PDI the information necessary to provision a security appliance configured specifically for Customer's environment. If a Customer has questions regarding the information or provisioning multiple sites, Customers may request a PDI Engineer to assist Customer.

Once the necessary discovery and onboarding information has been provided to PDI, PDI will initiate the provisioning and activation of the Service.

2.2. Deployment

Once all documents have been returned and confirmed by PDI, the PaySafe UTM Hardware is shipped directly to the location specified by the Customer during discovery. If necessary, the PDI project team will schedule a time and date with the Customer to guide the Customer through any pre-configuring required and with bringing the UTM online at the Customer site. The PaySafe UTM Hardware is shipped with basic installation instructions; Should the Customer have questions, PDI support is available 24x7x365 to assist.

2.3. Validation

After the initial deployment, PDI will work with the Customer to test the environment and ensure that it meets the Customer's access needs and published security policies.

3. **Services**

PDI's PaySafe UTM service consists of Managed UTM Services, UTM Software Licensing, UTM Hardware, and Cellular Connectivity.

3.1. Managed UTM Services

Managed UTM Service Components

3.1.1 Access Control Rules

3.1.1. Access Control Rules

For sensitive card holder network environments, PDI will develop access control rules that meet business needs while limiting or blocking all unauthorized or unneeded network traffic. PDI utilizes a "Deny by Default" security posture, limiting access to that which is explicitly authorized for the "CDE". "CDE" refers to processes and technology that store, process, or transmit cardholder data or sensitive authentication data. Upon request, PDI can apply restricted access controls to other network segments which are not part of the CDE.

3.1.2. Network Segmentation

PDI configures all PaySafe UTM's with network segmentation to protect sensitive card holder networks from local and public networks using clearly defined sub networking and accepted best practices for isolating and securing critical networks. This would be the initial configuration for any later Network Segmentation Validation Tests, as required under certain circumstances by the PCI DSS.

3.1.3. Health and Functionality

PDI utilizes automated alert systems in the event of changes in overall network health. These alerts include "online/ offline" primary connection alerts, automated failover and failback to secondary connections alert notifications.

3.1.4. IDS/IPS

Intrusion detection service (IDS) will detect and log potentially malicious network traffic based on defined rulesets. The intrusion detection feeds all packets flowing between local networks and Internet interfaces.

The Intrusion prevention service will automatically block potentially malicious traffic. Intrusion prevention's primary goal is to stop potential network attacks or unauthorized access before they are successful. All security events that trigger any IDS/IPS monitoring or action are immediately logged and available to view within the cloud based portal. These reports can be filtered by date/time, host, or event occurrence type.

3.1.5. Advanced Malware Protection (AMP)

PDI's UTM service includes malware protection technology. Malware detection screens the incoming and outgoing HTTP traffic for malware, trojan horses and phishing websites. Threats are detected and blocked based on either the URL or a signature triggered by the content. These services are updated daily, and all events logged and reviewable with the cloud-based portal.

3.1.6. Web Filtering

The UTM web filtering service allows customers the option to block certain categories of websites based on your organizational policies, example Peer to Peer, Sports, videos. In addition, whitelist and blacklist allow for additional customization to select web sites and/or website domains.

3.1.7. Site-to-Site VPN

Site-to-Site VPN allows for secure communications between 1 to many PaySafe UTM's. PDI

administrators will configure and monitor the availability of all site-to-site VPNs. This includes any troubleshooting required to allow users to successfully connect and stay connected through the service.

3.1.8. Group Policy Changes

Group policies define a list of rules, restrictions, and other settings, that can be applied to network segments in order to change how they are treated by the network. Any requests made for access, either during the initial deployment or ongoing once configuration has been completed, are assessed against existing PDI policies and published best practices. PDI Helpdesk will provide guidance to customers regarding these practices and help provide additional solutions that will still meet published security policies.

3.1.9. Content Tuning Policy

As customer requirements and needs change, PDI administrators will work to provide dynamic environments that meet any required compliance guidelines.

3.2. UTM Software Licensing.

PDI UTM Service includes pre-installed software with each hardware unit and includes a limited, nontransferable, royalty-free and nonexclusive license for Customer's use of such software during the term of the agreement.

3.3. Hardware

3.3.1. Warranty

PDI warrants for the term of the Agreement that Hardware will be free from defects in design, material and workmanship, conform to and perform in accordance with the documentation related to such hardware, if any, and function properly during the term of the Agreement. Customer's sole and exclusive remedy and PDI's sole and exclusive liability for any breach of this warranty is replacement of the defective hardware.

3.3.2. Maintenance and Return Policy

Maintenance for current hardware and software products consists of (i) repair, replacement or advanced exchange of the hardware, and (ii) related content updates, fixes and enhancements for the pre-installed software. Customer agrees to provide PDI with reasonable and safe access to any equipment purchased from PDI as necessary for PDI to perform these services.

If PDI concludes that the PDI-managed equipment has failed and is not restorable, PDI will use commercially reasonable efforts to ship a replacement unit to Customer by the end of the next business day and provide equipment self-installation support for the replacement equipment via the Helpdesk. Customer's license to use software on the defective hardware unit terminates at such time.

Customer must return the defective unit or components within two business days of receipt of the replacement unit or components. PDI will provide a pre-paid return shipping label for replacement or return shipments. Return must include all power supplies, antennas, and other components along with the original product box in the original shipping carton and packaging material. If this is not possible, use another shipping carton with padding to protect the units from damage during shipping. DO NOT ship a product without a carton. Customers will be charged for product that is damaged due to insufficient packaging or missing components.

Customer shall be liable for all charges and replacement costs attributable to the theft of any PDI or third-party owned equipment, or attributable to the loss of damage of such equipment due to intentional or negligent wrongdoing on the part of Customer or its employees.

3.3.3. Substitutes.

Whenever a material or piece of equipment is identified in an order, agreement or product description by reference to manufactures' tradename or model number, or the like, it is so identified for the purpose of establishing a standard, and PDI reserves the right at all times to substitute similar equipment where

interchangeability does not materially affect function.

3.3.4. Spare Hardware

A Customer may elect to have spare hardware on hand as replacement or in case of immediate need. In the event spare hardware is used, Customer will work with PDI support to swap equipment and provision replacement equipment. Upon termination of the Agreement, Customer will be responsible for shipping spare hardware.

3.3.5. Scheduled Maintenance

PDI may schedule maintenance outages for PDI owned equipment/servers which are being utilized to perform the services with 24-hours' notice to designated Customer contacts.

3.3.6. End of Life Hardware

PDI shall cease support for hardware on either the vendor's announced date for end of signature support, end of maintenance releases, or end of life, whichever comes first.

3.4. Cellular Connectivity

PDI offers two cellular connectivity services for customers for diverse connectivity or when a site is unable to order broadband.

3.4.1. PaySafe Cellular Failover

PaySafe Cellular Failover provides a seamless secondary cellular internet connection should the primary internet connection become unavailable. This service is intended for business-critical applications ONLY and not for general internet use.

- The PaySafe Cellular Failover service shall be used for back-up connectivity to the primary internet.
- It is solely for the use of payment related applications.
- Any other use of this service is strictly prohibited.
- Includes 300MB of data usage per month.
- Any use of this service except as intended may result in penalties including temporary suspension of cellular service and overage fees.

3.4.2. PaySafe Cellular Primary

PaySafe Cellular Primary access allows customers to choose cellular as the primary connectivity option where traditional land based broadband service is unavailable. The PDI representative will work with customers to determine the appropriate data plan.

- PaySafe Cellular Primary is billed monthly based on the site data plans provisioned in the boarding process
- All data sent or received using the cellular connection, including any network overhead associated with content sent or received, will be considered usage.
- Data transfer amounts will vary based on application; Customers may request assistance from PDI to determine the appropriate data plan.
- If data usage exceeds the provisioned amount, PDI may or may not provide immediate notice, and in any event, shall bill Customer for any charges resulting in excessive usage.

3.4.3. General Terms

CUSTOMER EXPRESSLY UNDERSTANDS AND AGREES that it has no contractual relationship whatsoever with the underlying wireless service provider or its affiliates or contractors and that the Customer is not a third-party beneficiary of any agreement between PDI and the underlying carrier. In addition, customer acknowledges and agrees that the underlying carrier and its affiliates and contractors shall have no legal, equitable or other liability of any kind to Customer and Customer hereby waives any and all claims or demands therefor.

4. **Out-of-Scope Services**

Services, deliverables and equipment not listed in the associated Service Order are out of scope and are not part of this particular Service. Any out-of-scope work may be completed by PDI after being defined in a separate, signed Statement of Work (SOW) upon your request. Out-of-scope items may include (but are not limited to):

- Professional Installation Services
- Support for any device or application not currently being managed by PDI, such as a modem provided by the Internet Service Provider (ISP).

5. **Security**

5.1. Network Environment

Upon installation, by Customer, the network activity and devices connected to the PaySafe UTM will be assessed by PDI. It will be determined by PDI that the standard configuration and network controls have been applied and the secure CDE is segmented from the non-CDE environment. PDI may recommend changes to Customer-provided devices to support the recommended segmentation. If Customer does not make recommended changes to its devices to achieve the segmentation as recommended by PDI, the network will be deemed unsecure and Customer will be advised, either by telephone call, email or letter that there is risk of non-compliance with PCI DSS. Customer acknowledges that it has responsibility for PCI DSS compliance and that a PDI determination that the network is secure does not act as a warranty or guarantee of security standard compliance nor is Customer relieved of its independent obligation to maintain PCI DSS compliance.

Only a Customer employee authorized to request changes to Customer's Network Design may request modification to the network, including adding devices or opening ports for access. Any change that impacts a secure segmentation requires written notice to PDI and Customer is fully responsible for any such requests and results therefrom. If the requested change will result in an unsecure network segmentation of the CDE, Customer will be so informed, and PDI reserves the right to deny any such request. In any case, all liability for the security of Customer-approved network will rest with Customer. PDI is responsible only for either (i) accommodating Customer's request or (ii) providing an explanation for denying such request. PDI will maintain records of the request, any advisement of risk and any authorization to make the change, particularly if it is against the advice of a PDI network engineer.

Customer is liable for securing the physical environment and securing physical access to all network components. Physical alteration of the network could create risk and PDI is not responsible for restricting access to the on-premise physical environment.

5.2. Cardholder Data.

PDI will comply with all applicable Payment Card Industry Data Security Standards ("PCI DSS") and acknowledges its responsibility for the security of cardholder data which PDI possesses, processes, or transmits on behalf of Customer as part of the Service being provided, or to the extent that it could impact the security of the Customer's cardholder data environment by its provision of the Service.

6. **Support**

PDI will be the primary interface for support for the services which are subscribed to, as indicated on Customer's Service Order.

6.1. Support Hours

PDI's managed security services Helpdesk is staffed 24x7x365. Customers can contact the support team via email or telephone to initiate troubleshooting and support.

6.2. Contact Information

Support for the PaySafe Services can be reached in the following ways:

- **Email**: mnfsupport@pdisoftware.com
- **Telephone**: 800-393-3246 Option 1

6.3. Authorized Users

PDI Support will only make configuration and profile changes if the change request is submitted by an authorized business contact. Customer's may request additional authorized users by completing the *PDI Dashboard Access Request form*.

Customer shall implement security procedures necessary to limit physical or other access to the PaySafe UTM Services to Customer's authorized users and shall maintain a procedure external to the PaySafe UTM Services for reconstruction of Customer's lost or altered files, data or programs.

Notwithstanding the foregoing, PaySafe UTM Services to which Customer may have access will be protected by password. In such a case, Customer shall (i) ensure that only its full-time personnel shall have access to any passwords provided by PDI for use by Customer in connection with the PaySafe UTM Services; (ii) not disclose such passwords to any third party except as permitted herein; (iii) be solely responsible for assigning roles and authority levels to its personnel with respect to its access and use of the PaySafe UTM Services; and (iv) be solely responsible and liable for ensuring that all third parties to whom Customer has granted access to the PaySafe UTM Services comply with all the terms and conditions of this Agreement. Customer acknowledges and agrees that it is solely responsible for strictly maintaining the confidentiality and integrity of all passwords provided by PDI or its suppliers. Customer shall notify PDI immediately in writing (or via email) if the security or integrity of any password or authority level has been compromised or if Customer becomes aware of any conduct by any of its authorized third parties that is in violation of the terms and conditions of this Agreement.

6.4. Contacting Support

When contacting PDI Security Operations for assistance, you will need to have the following information available so that we can efficiently assist you with your inquiry:

- **Business Name**: The name of the location calling in reference too.
- **Serial Number**: The number found on the bottom of the PaySafe UTM appliance.

6.5. Requesting Changes

After initial installation of the PaySafe UTM, all subsequent changes must be requested in writing using the PDI *PaySafe Firewall Change Request* form (provided by PDI support). This is required for tracking and audit purposes to ensure that all changes originated from an authorized representative of your organization. All changes will be reviewed to ensure the request does not violate PDI's secure configuration standards.

7. Customer Obligations

7.1. Customer either (i) owns and operates each Location or (ii) has authority to offer PDI PaySafe UTM Services and each Location. Customer is responsible for ensuring compliance with this Agreement for itself and each Location and is liable for such Locations' non-compliance, except to the extent a Location enters into an agreement directly with PDI for the PaySafe UTM Services.

7.2. Customer shall use the PaySafe UTM Services only for lawful purposes. Customer is solely responsible for the content of communications transmitted by Customer using the PaySafe UTM Services.

7.3. Customer, on behalf of itself and its Customer Locations, shall ensure (i) proper operating environments (ii) proper operation of the PaySafe UTM Services; (iii) compliance with all Payment Card Industry Data Security Standards ("PCI DSS") and/or any other applicable industry standard, as may be amended from time to time; and (iv) compliance with all applicable federal and state laws. In addition, Customer shall be solely responsible for obtaining and maintaining all hardware, software and services necessary for Customer-owned equipment.

7.4. Customer shall ensure that all Customer-owned equipment that connects to the PaySafe UTM Services will perform according to published technical specifications for such equipment and PDI's interface specifications. Customer shall be responsible for the use and compatibility of equipment or software not provided by PDI. This Agreement does not include the provision, maintenance, or repair by PDI of Customer-owned equipment or software, including, but not limited to, terminals, computer and other Customer third party equipment.

7.5. Customer grants PDI the right to electronically access the PaySafe UTM Equipment to provide, maintain and monitor the PaySafe UTM Services.

8. **Additional Service Terms and Conditions**

8.1. PDI reserves the right to modify the terms of this Service Description with 30 days' prior written notice.

8.2. Customers may also be subject to additional end user obligations posted at:

https://www.cisco.com/c/en/us/about/legal/privacy-full.html
https://cradlepoint.com/terms-of-service
http://www.verizon.com/about/terms-conditions/terms-of-use (for customers utilizing 4G Failover).
https://www.att.com/legal/terms.aup.html
https://www.sprint.com/legal/AUP.html