ArmorPoint

powered by trapp

ArmorPoint
Professional Services
and Service Add-Ons

Service Details

PROFESSIONAL SERVICES ADD-ONS

□ DEVELOP NETWORK DIAGRAMS

- ArmorPoint will provide customer with infrastructure and network access requirements
- ArmorPoint will run a scan to acquire list of Client network-connected assets
- The ArmorPoint team will create a high-level network diagram for purposes of implementing ArmorPoint into the Client environment
- **Client Requirements**
  - Provide ArmorPoint with complete infrastructure and network support
  - Provide required access to environment during scheduled window inclusive of permissions, virtual machines and network
- **Deliverables to be provided as part of this Statement of Work**
  - High-Level Network Diagram for the purpose of provisioning the physical out of band ArmorPoint Network Sensor

□ COMPILE NETWORK ADDRESSES

- ArmorPoint will provide Client with infrastructure and network access requirements
- ArmorPoint will scan the Client network to acquire available Client IP Addresses
- ArmorPoint will document network addresses including subnet masks and default gateways
- **Client Requirements**
  - Provide ArmorPoint with complete infrastructure support
  - Provide required access to environment during scheduled window inclusive of permissions, virtual machines and network
- **Deliverables to be provided as part of this Statement of Work**
  - Identified Client Internal IP Address, Subnet Mask, Network Gateway Address, DNS Server IP Address(es) and network device details to properly configure the physical out of band ArmorPoint Network Sensor

□ INCIDENT RESPONSE TABLETOP & PLANNING

ArmorPoint will lead and document Incident Response Plan training sessions and an Incident Response Tabletop exercise for Client to create an Incident Response Plan for crisis communication and escalation of major technology outages and cybersecurity incidents. Trapp Technology will work with Client’s Subject Matter Experts (SME) to identify and document processes best suited for their environment. Please refer to the scope and deliverable(s) listed below for complete project details.

Project Initiation and Management

- Review project scope and requirements with Client technology leaders.
- Identify specific team leaders and establish their specific roles.
- ArmorPoint to schedule meetings with the technology leaders and technicians for recovery planning team.
- Establish timelines for project milestones and project completion.
- Regularly report progress to the planning team.

Incident Management/Response and IT Escalation Strategies for Critical Services, Applications and Systems

- Review in place Communication and Incident Response solutions with Client leadership team(s).
- Review how problem management, knowledge management, business continuity, disaster recovery, and cybersecurity can be leveraged/impacted by incident management with Client IT leadership team(s).
- Based on discussions, determine which processes/resource roles should be called out in the Incident Management and Response plans.
- Review escalation processes and procedures to include in the plan.
- Develop initial Incident Response Plan implementation timeline.
- Provide templates and documentation for IR checklists, runbooks, and processes. Documentation to be completed while working with Client subject matter experts.
- Begin identifying and documenting the Incident Response options and escalation processes based on the in-place controls.
- Identify and define roles and responsibilities for recovery/response efforts of systems, networks, and identified critical services.
- Based on solutions determined by the Client project team, document the following:
    - Incident Response Plan.
    - Incident Response services and procedures.
    - Creation of an internal IT Communication and Incident Response Plan.
        - Documenting vendor contacts and escalation lists.
        - Documenting internal escalation lists and procedures to apply to incident response plan in ArmorPoint
        - Documenting site contact lists

Deliverables to be provided as part of this Statement of Work:

- Incident Response Plan document
- Incident Response Plan Workflow built in ArmorPoint SIEM solution
- Incident Response training sessions on Incident Response planning/processes

- Incident Response Tabletop Exercise

FULL SERVICE AGENT DEPLOYMENT

- The ArmorPoint team will provide automated deployment services of ArmorPoint and Managed Detection & Response (MDR) agents to in-scope machines
    - Windows device automated deployment of ArmorPoint agent will use Active Directory Group Policy Object (GPO) or PowerShell script
        - Active Directory Group Policy Object deployment process
            - Create Group Policy Object for ArmorPoint Agent
            - Edit a new GPO for automated deployment
            - Create task to run installation and start program
            - Link GPO to appropriate locations for finalization of deployment
        - PowerShell Scripting deployment process
            - Download ArmorPoint Agent Install Script
            - Execute Script using appropriate syntax
        - System Requirements:
            - Machine RAM: 4GB
            - CPU: Dual Core 2GHZ Core I3 equivalent and above
            - 1.5GB minimum available disk space
            - Network Connectivity: Ethernet or Wi-Fi
        - Network Requirements to be provided by Client:
            - Outbound TCP #### to 204.152.253.83 through 204.152.253.87
            - Outbound TCP 443
        - Installed Knowledge Base (KB) requirements to be provided by Client for each workstation:
            - KB2999226
                - Windows Server 2012 R2, Windows Server 2012
                - Windows Server 2008 R2 Service Pack 1(SP1)
                - Windows 8, Windows 8.1
                - Windows 7 SP1
            - KB3033929 or KB4474419
                - Windows Server 2008 R2 SP1
                - Windows 7 SP1

  - Windows device automated deployment of MDR agents will be by command line using standard installation feature and configuration parameters
    - System Requirements to be provided by Client for each workstation
      - Windows 10+
      - If using Windows 7, machine must have Windows KB3033929 or KB4474419 installed for SHA256 signature support
- Linux device deployment of ArmorPoint agent will use Linux terminal command line
    - System Requirements to be provided by Client for each workstation:
      - Machine RAM: 4GB
      - CPU: Dual Core 2GHZ Core I3 and above or equivalent
      - Available Disk Space: 1.5 GB minimum
      - Network Connectivity: Ethernet or Wi-Fi
    - Network Requirements to be provided by Client:
      - Outbound TCP #### to 204.152.253.83 through 204.152.253.87
      - Outbound TCP 443
  - Managed Detection & Response Agent:
    - Ensure proxy is setup on Linux machines
    - Download Linux installer file
    - Run commands to install agent to the machines
    - Provide support to ensure installed and checking in to portal
    - Linux requires Python 2.6+ or Python 3.0+ to be installed
- For MAC Devices, ArmorPoint will follow steps:
  - ArmorPoint Agent:
    - ArmorPoint will prepare agents for client for deployment
    - Confirm Intel/Apple Silicon
    - Download ArmorPoint Agent and enter customer specific ID and API Key
    - Run Installation Process
    - Provide troubleshooting support to ensure installed and checking in to ArmorPoint platform
    - System Requirements:
      - Machine RAM: 4GB
      - CPU: Dual Core 2GHZ Core I3 and above or equivalent
      - Available Disk Space: 1.5 GB minimum

            - Network Connectivity: Ethernet or Wi-Fi
        - Network Requirements:
            - Outbound TCP #### to 204.152.253.83 through 204.152.253.87
            - Outbound TCP 443
    - Managed Detection & Response Agent:
        - ArmorPoint will prepare agents for Client deployment
        - Download of .pkg installer package
        - Software distribution tool will install the .pkg installer on endpoints
        - Provide support to ensure agents installed and checking in to ArmorPoint platform
- **Client Requirements**
    - Provide ArmorPoint with complete infrastructure support
    - May require administrative access for ArmorPoint team to perform needed steps for install
    - Full access to environment during scheduled window inclusive of permissions, virtual machines and network

AUTOMATED AGENT DEPLOYMENT CONSULTING

- ArmorPoint will provide remote engineering ad-hoc hourly consulting and support to attend working sessions with Client to plan automated agent deployment
- ArmorPoint will provide remote engineering ad-hoc hourly consulting and support to assist Client with environment preparation for automated agent deployment
- The ArmorPoint team will provide remote engineering ad-hoc hourly consulting and support for troubleshooting during the automated agent deployment
- ArmorPoint team recommends the following deployment methods for Windows:
    - 1 – Remote Monitoring & Management (RMM) Tool
    - 2 – Active Directory Group Policy Object (GPO)
    - 3 – PowerShell Script
- Remote engineering consulting and support is available Monday through Friday from 8:00 AM to 5:00 PM Mountain Standard Time

ARMORPOINT DEPLOYMENT CONSULTING FOR PROXY OR PRIVATE ENVIRONMENT

- ArmorPoint will provide remote engineering ad-hoc hourly consulting and support to attend working sessions with Client to plan event log forwarding and agent deployment solution for

Proxy or Private Environments (examples include: Virtual Desktop Infrastructure, Public or Private Cloud Environments, etc.)

- ArmorPoint will provide remote engineering ad-hoc hourly consulting and support to assist Client with environment preparation for event log forwarding and agent deployment solution
- Remote engineering consulting and support is available Monday through Friday from 8:00 AM to 5:00 PM Mountain Standard Time

□ SYSLOG FORWARDING

- Ensure all prerequisites are met for client environment
- Create and configure syslog profiles
- Configure syslog forwarding
- Update firewall rules to allow remote administration
- Increase log size for Forwarder Events
- Complete testing and confirm solution is operational
- **Client Requirements**
  - Provide ArmorPoint with complete infrastructure support
  - Full access to environment during scheduled window inclusive of permissions, virtual machines and network
  - Provide access to network administrative rights to allow forwarding to ArmorPoint network sensor

□ WINDOWS/LINUX EVENT LOG FORWARDING

- ArmorPoint will provide remote engineering consulting and support to deploy Windows/Linux Event Log Forwarding solution by Active Directory Group Policy Object or other means for Linux
- Define prerequisites and task ownership for Client environment to support Windows/Linux Log Forwarding solution
- Complete defined prerequisites for Client environment
- Create and/or confirm required Active Directory Organizational units
- Create Group Policy Objects
- Edit Group Policy Object to allow remote server management through WinRM
- Enable Windows Remote Management for Group Policy Service and Start
- Update firewall rules to allow remote administration
- Create new GPO to apply Windows Event Log Forwarding Settings
- Link GPOs and enable WinRM and Event Log Forwarding
- Enable Subscription Collector Service

- Increase log size for Forwarder Events
- Complete testing and confirm solution is operational
- **Client Requirements**
  - Client will designate a single point of contact responsible for directing and providing resources and information to the ArmorPoint team
  - Client will provide ArmorPoint team with complete infrastructure support
  - Client will provide required access to environment during scheduled window inclusive of permissions, virtual machines and network
- Remote engineering consulting and support is available Monday through Friday from 8:00 AM to 5:00 PM Mountain Standard Time

FULL SERVICE NETWORK SENSOR INSTALLATION

- ArmorPoint will configure the network sensor(s) with Client-provided internal IP Address, Subnet Mask, Network Gateway Address, DNS Server IP Address(es)
- ArmorPoint will schedule an onsite Network Engineer once receipt of network sensor(s) is confirmed at Client location(s)
- Client network administrator be responsible to work with the Network Engineer to set outbound access requirements for network sensor
- ArmorPoint Network Engineer will install network sensor in designated rack provided and prepared by Client
- The Network Engineer will configure Mirror/SPAN port on Client switch
- ArmorPoint Network Engineer will connect network sensor to Client switch LAN and configured Mirror/SPAN ports in out of band installation
- The Network Engineer will provide guidance or whitelist appropriate ArmorPoint IP's addresses and URL's
- The Network Engineer will confirm successful network sensor installation and validate network traffic
- **Customer Requirements**
  - Receipt and storage of ArmorPoint network sensor(s) for handover to onsite ArmorPoint Network Engineer
  - Provide ArmorPoint with complete infrastructure support
  - Provide required access to environment during scheduled window inclusive of permissions, virtual machines and network
- ArmorPoint Network Engineer and support is during standard business hours, Monday through Friday from 8:00 AM to 5:00 PM Mountain Standard Time

□ SPAN PORT CONFIGURATION

- Port mirroring (or SPAN) is a method used on network devices to send a copy of network traffic to ArmorPoint SIEM for correlation, analysis and alerting
- ArmorPoint will work with client to gain access to network devices needing SPAN Port Configuration
- ArmorPoint will work to connect internal network devices to the network sensor
- ArmorPoint team will utilize best practice recommendations per customer network in order to configure Mirror/SPAN interface
- ArmorPoint team will validate network traffic routing to ArmorPoint when SPAN is configured
- ArmorPoint will provide any troubleshooting during process and may make recommendations to customer to make additional network changes
- ArmorPoint will make network changes per customer best practice and change management process
- **Customer Requirements**
    - Provide ArmorPoint with complete infrastructure support
    - Provide required access to environment during scheduled window inclusive of permissions, virtual machines and network

□ CUSTOM REPORT CREATION

- ArmorPoint will build (1) custom report in ArmorPoint SIEM
- Client will provide necessary rationale and requirements for custom report
- ArmorPoint will review available fields and reportable data with Client for report build
- ArmorPoint will design and build custom report per customer requirements
- ArmorPoint will provide (1) iteration review with Client for report edits
- Client will determine the report generation frequency for ArmorPoint to setup
- ArmorPoint will perform a final review and sign-off with Client
- ArmorPoint will publish report to Client instance

□ CUSTOM DASHBOARD CREATION

- ArmorPoint will build (1) custom dashboard in ArmorPoint SIEM
- Client will provide necessary rationale and requirements for dashboard
- ArmorPoint will review available fields and reportable data with Client for dashboard creation
- ArmorPoint team will design and build dashboard per customer requirements
- ArmorPoint will provide (1) iteration review with Client for dashboard edits

- ArmorPoint will perform a final review and sign-off with Client
- ArmorPoint will publish dashboard to Client instance

□ COMPLIANCE/AUDIT DOCUMENTATION ASSISTANCE

- ArmorPoint team will provide remote ad-hoc hourly support to prepare evidence for Client-requested compliance/audit requirements. Evidence can include exports of logs, events, alerts, incidents or documentation.
- ArmorPoint does not guarantee all evidence requests can be satisfied and will work on a best effort basis.
- Client will be responsible for hours of effort regardless of ArmorPoint's ability to deliver requested evidence.

□ VULNERABILITY SCANNING SETUP

- ArmorPoint team will work with Client to setup dedicated vulnerability scanner
- ArmorPoint will work with Client to gather necessary requirements for internal and external scanning
  - External Scanning: External-facing IP addresses and subnets; Public-facing owned URLs
  - Internal Scanning: Internal IP addresses and subnets by monitored location; Username, Domain and Password used for credential based scanning.
  - Exceptions or excluded IP addresses
- ArmorPoint will provision scanner to provide external scanning and internal scanning
- ArmorPoint will set monthly scanning cadence after consultation with client on preferred scan schedule
- Monthly review meeting of results can be provided ad hoc per billable invoice
- All management or remediation of vulnerabilities are excluded
- **Customer Requirements**
  - Provide ArmorPoint with complete infrastructure support
  - Provide exceptions or IP addresses that should be excluded
  - Provide required access to environment during scheduled window inclusive of permissions, virtual machines and network

- **Deliverables to be provided as part of this Statement of Work**
  - Report with scan results and findings delivered into ArmorPoint's SIEM Report section.

□ STANDARD ARMORPOINT INTEGRATION SETUP

- ArmorPoint team will assist Client perform data ingest connection to self-service integration.
    - ArmorPoint will provide working session with Client to review integration setup documentation and provide guidance for configuration of Client tool to ingest data into ArmorPoint
    - Client will perform Client tool configuration required for ArmorPoint to ingest Client data
    - ArmorPoint will perform ArmorPoint Platform backend configuration required to ingest Client data
    - ArmorPoint will validate data is collected, ingested and delivered into ArmorPoint Platform
    - Client will validate required data is accurate and present in ArmorPoint Platform
- Deliverable: Ingested data from Client data source to ArmorPoint Platform

CUSTOM INTEGRATION DEVELOPMENT

- The ArmorPoint team will provide a dedicated Project Manager and development team to perform the following:
    - Review Client requirements for data ingestion into ArmorPoint SIEM
    - Work with Client to design required API functions
    - Develop API to integrate into ArmorPoint
    - Create panels and dashboard in ArmorPoint SIEM
    - Validate data is collected, ingested and delivered into ArmorPoint Platform
    - Publish standard dashboard, report, and alert rules in ArmorPoint Platform
- Client Requirements
    - Provide ArmorPoint development resource with required sandbox access to develop API
    - Validate required data is accurate and present in ArmorPoint Platform

- Deliverables to be provided as part of this Statement of Work
    - Ingested data from Client data source to ArmorPoint Platform
    - Standard dashboard, report, and alert rules in ArmorPoint Platform

ARMORPOINT PLATFORM TRAINING

The objective of the below ArmorPoint training proposal is to provide Client with extended training for successful understanding and usage of the ArmorPoint Platform.

ArmorPoint and Client will collaborate to develop a training program for the Client team.

- 10 hours of ArmorPoint training per month, to be billed at $200 per hour on a monthly/annual cycle, totaling $2,000 per month for (1) number months.

- 4 of the 10 hours per month will be dedicated to a weekly recurring ArmorPoint Training and Support call attended by an ArmorPoint resource for:
    - Configuration Support
    - Best Practice Guidance
    - Technical Guidance & Recommendations
    - Troubleshooting
    - Incident Event Review & Guidance
    - Overall Product Training
- 6 of the 10 hours will be dedicated to 2-hour working sessions for:
    - Incident or Alert Escalation (priority on Network Events)
    - Configuration Review
    - Dashboard Training
    - Reporting Guidance
    - Operational Guidance
- Requests from Client for 2-hour working sessions will have a 48-hour SLA for the ArmorPoint team to respond with available windows for ArmorPoint training team

□ NETWORK ARCHITECTURE & BEST PRACTICE CONSULTING

- ArmorPoint will provide networking ad hoc hours for network architecture and implementation best practice consulting to maximize security posture for client

ONGOING SERVICES ADD-ONS

□ MANAGED NETWORK

- Managed Server
- Managed Firewall
- Managed Switch
- Managed Access Point
- Managed Router
- Managed VPN Tunnel

Services below include monitoring, management and patching services for the following:

- Client dashboard, alerts and notifications including tickets generation and management

Network equipment must have an active support contract in place and not be End of Life (EOL).

Monitoring

Monitoring shall be provided 24x7x365. This includes internal escalation procedure to ensure issues are resolved based upon Service Level Agreement.

Services include provision of the following:

- 24x7x365 real-time availability and performance alerting and notification.
- Up/Down state monitoring and relevant connectivity
- Operating system monitoring including CPU, memory utilization, disk space, system and connectivity
- Backup of configuration data for in-scope network devices
- Technical assistance to Client on 3rd party vendor calls and issues when it interfaces with ArmorPoint's in-scope services

Patching

Patching services are performed per ArmorPoint's pre-defined schedule for supported infrastructure. ArmorPoint will perform patching and updates during a scheduled maintenance window with coordination and pre-approval by Client.

ArmorPoint will manage key patches of in-scope infrastructure components to maintain the current security level of Client.

- Windows OS Patching: Third-party updates and patching is not included.
- Weekly Maintenance occurs every Tuesday from 8:00 PM to 11:59 PM Arizona Time.

Infrastructure Management

Management shall be provided 24x7x365. This includes internal escalation procedure to ensure issues are resolved based upon Service Level Agreement.

Services include provision of the following:

- Major release updates are not included for firmware and OS operating system upgrades.
- Trapp Technology is responsible for troubleshooting and remediation of failed Trapp Technology provided software/hardware.
- Client is responsible for providing all policies including configuration, rule sets, alert notification, remediation, and patching/firmware updates to Trapp Technology.
- Upon client request, Trapp Technology may perform moves, adds, or changes to the network devices. Moves, adds, or changes on the behalf of the Client will facilitate through the Trapp Technology support desk and ticketing system.
- Isolation, troubleshooting, remediation of issues resulting from a client requested configuration change will be included.
- It is recommended that client maintain a strategy for intrusion detection and prevention including corporate policies, security policies, or firewall rule sets. Upon request by client, Trapp Technology is available to review client's policies.

- As-built documentation, maintenance and updates are the responsibility of the client. Trapp technology can assist per billable support rates.

Incident Response

- ArmorPoint Incident Response services are invoked upon confirmation of an Incident. Incident Response may include the creation of new or update of existing firewall policies by the ArmorPoint Service Operations Center (SOC) Team.
- The ArmorPoint team will provide documentation of all Incident Response activity. Reporting will include information on how the Incident was identified, the impact of the Incident, any person(s) notified of the Incident, and steps taken to remediate the Incident.

□ VULNERABILITY SCANNING (MONTHLY)

The vulnerability scan will focus on safeguarding Client's information and systems from threats and vulnerabilities including, but not limited to; configuration, open ports and ratings of vulnerabilities. This will produce an analysis of Client's security posture by conducting vulnerability scanning against the identified Client systems.

The findings will enable Client to operate, plan, and secure the infrastructure and applications in accordance with data security standards.

External and Internal Scanning

- Using automated processes, ArmorPoint will conduct external vulnerability scanning to identify client's external vulnerabilities.
- Vulnerability testing and scanning on external/internal networks and systems (DMZs), and any external network connection points.
- Provide documentation and recommendations for remediating identified vulnerabilities from the vulnerability scan.
- Recommendations will be provided based on priority (Critical, Severe, High, Medium, Low).

Deliverables to be provided as part of this Statement of Work:

- Report with scan results and findings based on criticality and remediation recommendations will be delivered into ArmorPoint's Report section.

□ DARK WEB MONITORING INTEGRATION & SERVICE

- ArmorPoint will provide data points for the following across the open, deep and dark web:
  - Dark Web Monitoring: Uncover cyber threats across dark networks and messaging apps
  - Data Breach Detection: Detect compromised personal and company info widely available on the web
- Deliverable: Monthly Report with findings from Dark Web Monitoring & Data Breach Detection data feeds.

SECURITY REPUTATION MONITORING

ArmorPoint will provide a monthly report outlining current client security rating.

- Provide visibility into key areas of cyber risk that are correlated to breach, including Compromised Systems, Open Ports, Mobile and Desktop Software, and File Sharing Provides reporting on peer and sector-wide security benchmarking
- Provide monitoring for Client and third party's security rating changes. This monitoring is for one domain.
- Deliverable: Monthly Report on Client's reputation score compared to their industry peers. Report will consist of full company report with all findings.

□ SPAM FILTERING – OFFICE 365

Spam Filtering for Office 365 to be deployed with the following values:

- AI-based solution effective in detecting spear-phishing attacks and preventing account takeover
- Automated Incident Response and Remediation Solution minimizes damages and costs, provides actionable forensic insights
- Spam and Malware Protection
- Email Encryption
- Data Loss Prevention

□ SPAM FILTERING – EMAIL

Spam Filtering for Email Security to be deployed with the following values:

- Advanced threat protection, encryption and data loss prevention
- Real-time detection for dynamic threat analysis with 24x7 updates and protection
- Link protection deters targeted phishing and spear phishing attacks
- Outlook plug-ins and mobile apps for easy user access
- 100% cloud-based: No hardware or software required
- Centralized cloud-based management console

□ DOMAIN NAME SYSTEM (DNS) SECURITY

DNS security services to be deployed and configured on Client desktops and laptops. Policy will be determined by Client.

- Blocks domains with malware, phishing, botnet and other high risk items
- Custom block/allow lists of domains
- Enable web filtering by domain or category
- Forward external DNS for on-network coverage and off-network devices

- Real-time activity search, plus reporting API to extract key events

□ ADDITIONAL LOG RETENTION (12 MONTH INCREMENTS – ARCHIVED & RETRIEVABLE)

ArmorPoint will provide additional log retention services hosted in ArmorPoint's SOC II Type II compliant data center. The additional storage of logs can be purchased in 12 month increments. All logs/data will be stored in cold storage.

□ INTEGRATIONS

ArmorPoint will collect event data from in-scope external systems via API or syslog. This information will be integrated into the SIEM Dashboard for insight into the environment.

ArmorPoint will develop and maintain API's for the following supported tools:

- Microsoft Office 365
- 1Password
- ArmorPoint Dark Web Monitoring
- Amazon Web Services
- Microsoft Azure
- Cisco Duo
- Cisco Umbrella
- Citrix ShareFile
- CloudFlare
- CrowdStrike
- GitHub
- Google Cloud Platform
- Okta
- PaloAlto Cortex XDR
- Tenable.Nessus
- Tenable.SC

□ APPENDIX A: MANAGED NETWORK SLAS

SERVICE LEVEL AGREEMENT – MANAGED NETWORK SLA

The following constitutes the reference for performance and expectations regarding Managed Network SLAs.

Business Hours – 24x7x365

SUPPORT HOURS

24x7x365 excluding maintenance windows and emergency repair operations. During this time, Client IT assets and performances will be monitored and interventions will take place should an exception occur. Client users will be able to access the ticketing portal and submit tickets for Incidents and Service Requests, with the exception of the Maintenance Window.

Weekly Maintenance occurs every Tuesday from 8:00 PM to 11:59 PM Arizona Time.

Trapp Technology Support Hours are 8:00 AM to 5:00 PM Arizona Time, Monday through Friday. All support beyond these hours are classified as “After Hours.”

Service Guidelines

The Trapp Technology Service Desk uses a Triaged Response Metrics system to prioritize Client Incidents. The below Triaged Response Metrics outlines our standard service level commitments for communicating the Incident status to Client.

Response time commitments do not promise a complete resolution within the stated time frames, rather the time commitment is intended to indicate the maximum time interval in which the client will be contacted by a Trapp Technology Service Desk Representative.

Priority Definitions:

Priority of a ticket is defined by Severity, Impact and Urgency. Impact and Urgency are determined according to the chart below and assigned by Trapp Technology:

- Tertiary System – Systems that have little impact on normal day-to-day operations.
- Secondary System – Systems where a service interruption would have a moderate impact on operation of business.
- Core Business Service - Systems where a service interruption would have significant impact on the daily operation of business.

Ticket Level Definitions:

Level 1 – Initial support level responsible for basic client issues including but not limited to basic troubleshooting, resolving username and password problems, basic access issues, verification of proper hardware and software setup.

Level 2 – More in-depth technical support level than Level 1 as more experienced and knowledgeable technicians are required to support the incidents and/or problems. Level 2 technicians are responsible for assisting Level 1 personnel in solving basic technical problems and for investigating elevated issues by confirming the validity of the problem and seeking known solutions for these more complex issues. This may include, but is not limited to, replacements of various hardware components, diagnostic testing and utilization of remote control tools used to take over a machine for the sole purpose of troubleshooting and finding a solution to a problem.

Level 3 – The highest level of support in a three-tiered ITSM technical support model responsible for handling the most difficult or advanced problems. Level 3 technicians are experts in the field and responsible for not only assisting Level 1 and 2 technicians but with the research and development of solutions to new or unknown issues. It is typical for a developer or someone with knowledge of code or backend infrastructure to be a Level 3 technician. Level 3 technicians are responsible for designing and developing one or more courses of action, evaluating each of these courses in a test case environment and implementing the best solution to the problem.

	Urgency		
Impact	Tertiary System	Secondary System	Core Business Service
All users	High	High	Critical
Group of users	Medium	High	Critical
One User	Low	Medium	High

General Service Targets

PERFORMANCE TARGETS

Triaged Response Metrics:

	Priority Rating							
Stage	**Critical**		**High**		**Medium**		**Low**	
	Phone	Chat	Phone	Chat	Phone	Chat	Phone	Chat
1. Initial Response								
	1 Hour	1 Hour	2 Hours	2 Hours	4 Hours	4 Hours	8 Hours	8 Hours
2. Plan Within								
	2 Hours	2 Hours	4 Hours	4 Hours	8 Hours	8 Hours	24 Hours	24 Hours
US Observed Holidays	2 Hours	2 Hours	8 Hours	8 Hours	Next Business Day	Next Business Day	Next Business Day	Next Business Day
3. Resolution Response	**Incl.**	**Incl.**		**Incl.**		**Incl.**		**Incl.**
4. Resolution Target	**Best Effort / ASAP**		**8 Hours**		**24 Hours**		**48 Hours**	
5. Closure Response	**Incl.**	**Incl.**		**Incl.**		**Incl.**		**Incl.**

These Service Details may change and ArmorPoint may update this document from time to time. It is your responsibility to check this periodically for changes.

Exclusions

The following exclusions apply to the scope of the work stated above and have been incorporated into the pricing stated below:

- Any work or services not expressly provided for herein
- Any application development or integration efforts not expressly provided for herein
- Any actual hardware purchases for on-premise needs
- Any migration or upgrade of infrastructure (servers, network, etc.)
- Any actual implementation of the recommendations made by ArmorPoint unless specified in this document
- Any efforts tied to re-installing OS due to virus or malware or any system instability after the removal of a virus
- Any work related to being crypto-locked. ArmorPoint will work to mitigate the spread by blocking at the edge and/or taking machines offline
- Any data recovery and forensics work due to purposeful or malicious Client or application errors
- Any software license or physical hardware expenses
- Any software license that’s not explicitly mentioned, and not covered by ArmorPoint
- All Travel and lodging costs
- Any fees related to shipping, handling, customs, duties and/or taxes
- Any additional work requested beyond the scope of this Agreement will be expressly set forth by subsequent agreement, including, but not limited to, a Contract Change Request (“CCR”)

This SOW may change and ArmorPoint may update this SOW from time to time. It is your responsibility to check this SOW periodically for changes.

REVISION DATE: 08/23/2022