Managed Risk

Statement of Work

ArmorPoint Managed Risk Service Scope

RISK ASSESSMENT WORKSHOP

ArmorPoint will provide a detailed risk workshop to help Client understand business risks and the impact/s associated; the workshop will consist of involved technical discussions with a technology advisor.

KICK-OFF MEETING:

- 30-minute discussion to introduce ArmorPoint advisor & objectives
- Discuss and set the agenda for the workshop
- Schedule and on-site or off-site workshop, including date and time

WORKSHOP MEETING:

- A dedicated, half-day discussion with Client key-stakeholders to deep dive into existing tools, services, policies and processes, including:
    - Business Continuity and Disaster Recovery
    - Incident Response and Security Management
    - Risk Mitigation Strategies
    - Crisis Communication
    - Process Management

DELIVERABLE REVIEW MEETINGS:

- ArmorPoint's technology advisor will present key findings, identified gaps, and recommendations that support Client's stated business requirements and goals.
- Review actionable items to help guide Client towards a secure and risk-aware environment.
- Present comprehensive documentation designed to assist Client and executives in making informed decisions to mitigate risks.
- Any remediation of vulnerabilities or findings is not included in this service.

SECURITY REPUTATION SERVICES

ArmorPoint will provide 24x7x365 Security Reputation Monitoring Services. The following will be included with these services:

- 24x7x365 Security Monitoring Services for (1) one domain
- One (1) Monthly detailed report
- Industry comparison reporting
- 24x7x365 Security Alerting
- Monthly remediation reporting
- Any remediation of vulnerabilities or findings is not included in this service.
- Any additional work or services requested beyond the scope of this Agreement shall be expressly set forth by subsequent agreement including, but not limited to, a Client Change Request (CCR).

SECURITY AWARENESS TRAINING

ArmorPoint has developed an information security awareness curriculum that includes the following:

- Access to a dedicated training portal for employees who fail phishing email campaigns
- Real-time reporting and measurement on progress of employees enrolling, progressing and completing security awareness training program
- Several Security Training Courses included
- Training videos and quizzes required to successfully complete program
- Monthly automated Phishing tests and quarterly User Awareness trainings to be pre-scheduled with Client
- A minimum of 2 weeks advance notice is required from Client to request and schedule a Phishing Campaign or User Awareness Trainings.

MONTHLY EMAIL PHISHING CAMPAIGNS + PHISHING REMEDIATION

ArmorPoint will evaluate the security awareness of Client end-users through means of a social engineering assessment. The social engineering assessment will seek to determine how susceptible staff members are to phishing attacks:

- ArmorPoint will collaborate with Client to Determine appropriate phishing campaign strategies for monthly testing, including scenario-based strategies.
- Campaign phishing emails will direct Client end-users to a URL which logs click-through rates and the originating end-users.
- Phishing emails will provide real-time coaching to end-users on how to spot future phishing emails.
- After each monthly campaign, Client will have access to real-time reporting metrics and all end-users that engage with the campaign will be enrolled in a security awareness program.
- Client will be provided the means to setup a process for end-users to report suspected phishing attacks to the ArmorPoint SOC:
    - The ArmorPoint SOC will review the reported emails to determine if the email is safe or malicious

- For emails determined to be malicious, when applicable, and if the client has the proper process establish, the SOC will initiate remediation steps to remove the email from end-user inbox

QUARTERLY USER AWARENESS TRAINING

ArmorPoint offers automated virtual User Awareness Training Services as part of a comprehensive security awareness program to educate Client employees about cybersecurity and cyber threats.

- Quarterly User Awareness Training campaigns that can be pre-scheduled by Client on a quarterly basis.
- Client will assign and provide a User Awareness Training Manager as a main point of contact for scheduling, coordinating, and communicating User Awareness Training Sessions with Client employees.
- At the conclusion of each User Awareness Training, Client will be provided insights into end-user scores, pass/fail metrics, and areas of improvement needed.

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 on a pre-scheduled monthly basis; scheduling will be determined at time of implementation project.
- 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).

VULNERABILITY MANAGEMENT GUIDANCE

- Client has access to the ArmorPoint Security team to seek guidance on vulnerability management strategy, including:
  - Vulnerability prioritization
  - Risk acceptance of vulnerabilities
  - Guidance on vulnerability management practices
  - Guidance on patching practices
- ArmorPoint will provide an optional monthly meeting to discuss the most recent vulnerability scan/s and offer guidance to Client on newly discovered vulnerabilities.

- Any remediation of vulnerabilities or findings is not included in this service.
- Any additional work or services requested beyond the scope of this Agreement shall be expressly set forth by subsequent agreement including, but not limited to, a Client Change Request (CCR).

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.
- If optional monthly meeting is held, ArmorPoint will deliver a prioritization document of newly found vulnerabilities.

BREACH & ATTACK SIMULATION (MONTHLY)

The breach and attack simulation (BAS) scan will safely conduct threat activities via pre-built testing scenarios based on various security control best practices, MITRE & NIST mappings, and full kill-chain scenarios to test and validate Client's existing security controls and measure Client's security posture.

The findings will enable Client to understand their threat landscape and security posture maturity in accordance with data security standards.

BREACH & ATTACK SIMULATION SCAN

- Using automated processes, ArmorPoint will conduct a monthly attack scenario on behalf of the Client to test their existing security posture, including:
    - Endpoint Protection Platform (EDR/AV)
    - Web Content Filtering
    - Next-Gen Firewall
    - SIEM/DLP Capabilities
- BAS scanning on internal/external infrastructure, including networks and devices
- Provide documentation and recommendations for remediating identified security gaps or weaknesses from the BAS scan, including:
    - Misconfigured Controls
    - Coverage Gaps
    - Missed Detections
- Recommendations with be provided based on priority

DELIVERABLES TO BE PROVIDED AS PART OF THIS SERVICE AGREEMENT:

- Report with scan results and finding based on criticality and remediation recommendations with by delivered into ArmorPoint's report section.

- Hands-on remediation is not included within this agreement; if any remediation work is needed, the execution of a CCR is needed.

CONTRACTUAL CHANGES

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.

The following Governance structure defines the Contract Change Process:

Change To	Vehicle	Process
Service scope	Change of scope presented with justification and supporting data. Changes that cause a change to the monthly cost to Client of more than $1,000 will require further Executive Approval through a Contract Change process.	Order Form
New project or effort	Each proposed effort or initiative will be presented to executive leadership and/or board with supporting charter, solution outline and estimates.	Order Form
Change to the overall service requirements and performances	Each change will be presented to the Executive and be processed with further Executive Approval	Contract CCR or Addendum
Change to the scope, terms, and conditions of the current	Each change will be presented to the Executive and be processed with further Executive Approval	Contract Addendum

EXCLUSIONS

The following exclusions apply to the scope of the work stated above and have been incorporated as assumptions 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 Trapp Technology 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. Trapp Technology 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 Trapp Technology
- All Travel and lodging costs.
- Any additional work requested beyond the scope of this Agreement will be expressly set forth by subsequent agreement, including, but not limited to, a Client Change Request ("CCR").

APPROVAL AND AUTHORIZATION

This Agreement shall be binding and effective as of the date upon which both Parties being fully authorized have signed. This Agreement may be executed simultaneously in one or more counterparts, each of which shall constitute one and the same instrument.

ARMORPOINT

(Name)	(Title)
(Signature)	(Date)

CLIENT

(Name)	(Title)
(Signature)	(Date)

ATTACHMENT A – RATE SCHEDULE

In addition to the amounts set forth above, any technical support provided by ArmorPoint in connection with the services shall be billed by ArmorPoint on a time and materials basis pursuant to the following rate schedule.

- All fees are in US Dollars.
- Incident Response as well as data and/or application migration services are available upon request for an additional fee/cost.

Remote Support (1 hr. min, billed in 15-minute increments)

Project Coordinator	$95 per hr.
Program or Project Manager	$155 per hr.
Engineering Consultant	$185 per hr.
Sr. Engineering Consultant	$210 per hr.
Engineering Architect Consultant/Application Architect Consulting	$225 per hr.
Incident Response Consultant	$275 per hr.

On-Site Scheduled Support (8 hr. min, scheduled 24 hrs. in advance)

Data Cabling/Desktop/Printer	$95 per hr.
Engineering Consultant	$195 per hr.
Program or Project Manager	$160 per hr.
Sr. Engineering Consultant	$225 per hr.
Engineering Architect Consultant/Application Architect Consulting	$250 per hr.