Aberrant Open-ISM™

SERVICE PROVIDER MANAGEMENT POLICY

Property	Description
Document Version	1.0
Status	DRAFT
Last Update	2022-03-25
Document Owner	Risk Management
Next Scheduled Review	

Document Approvals		
Approver Name	**Title**	**Date**
???	???	???

Revision History			
Version	**Date**	**Description of Changes**	**Revised by**
1.0	2022-03-25	DRAFT	Aberrant

TABLE OF CONTENTS

1 OVERVIEW

This policy provides a framework for how <<Company Name>> interfaces with service providers—also know as vendors. The purpose of this policy is to provide explicit instruction for how we manage relationship with third parties.

2 SCOPE

This policy applies to service providers. Namely, selection, evaluation, onboarding, monitoring, and offboarding.

3 SERVICE PROVIDERS

3.1 SELECTION

The selection of operational systems requirements spending approval from executive management and should be evaluated against ROI and other company priorities.

3.1.1 NON-DISCLOSURE AGREEMENT (NDA)

Prior to any discussion that involves <<Company Name>> proprietary information a NDA should be in place and stored in the system.

3.1.2 SYSTEM REQUIREMENTS

System requirements should be clearly communicated to the vendor in order to ensure that requirements are included in the contract prior to signing. Some examples of system requirements:

- System uptime
- Acceptable request latency within two standard deviations.
- Acceptable error rates / error budget.
- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)

3.1.3 SECURITY REQUIREMENTS

Security requirements should be clearly communicated to the client and should be validated against the NDA. Some examples of security requirements:

- ISO/IEC 27001:2013 certification; a SSAE 18 SOC 2 Type 2 Report; etc.
- Breach notification

- Annual penetration testing

3.2 EVALUATION

3.2.1 VALIDATION OF AUTHENTICITY

The Service Provider should be evaluated to ensure that it's an authentic company. Review of the service providers articles of incorporation, client references, financials, etc. should be used to verify whether or not a service provider is authentic.

3.2.2 NON-DISCLOSURE AGREEMENT (NDA)

Prior to sharing detailed information with a Service Provider an NDA must be in place. All NDAs must undergo legal review prior to approval.

3.2.3 SERVICE PROVIDER CONTRACTS

Contracts received from a service provider should undergo legal review to ensure that they conform to system and security requirements. Contracts should delineate:

- scope of service;
- roles and responsibilities;
- confidentiality requirements;
- support requirements;
- security requirements: e.g. data handling, breach notification, required certifications, penetration testing, etc.;
- boundaries of the system and describes relevant system components;
- communicates the system commitments and requirements of third parties;
- outlines and communicates the terms, conditions and responsibilities, including those relating to confidentiality;
- address general requirements such as termination, "Force Majeure", termination clause, etc.; and,
- liability;

Additional contract provisions should be assigned based on a CVSS score from a risk evaluation of the service provider. Please see Appendix A for a matrix of contract provisions based on the service provider's CVSS score.

3.2.4 PROOF OF CONCEPT (POC) TESTING

Optionally, a product evaluation, or proof of concept should be performed to ensure that the application works as designed prior to deploying the system in a production environment. A

POC test requirement falls within the purview of the CTO. The product owner should also have input into this decision.

3.3 SERVICE PROVIDER ONBOARDING

Service Providers should be evaluated against a check-list of requirements to ensure that they are onboarded consistently. The checklist should include:

- A signed MSA
- An LOI if the deployment is scheduled into the future.
- Payment information for Accounts Payable—e.g. entry into the ERP system.

3.3.1 CATALOGING AND CLASSIFICATION

When a service provider is onboarded they should be documented in a service provider catalog, or inventory. The following information should be inputted:

- a product owner (e.g. the <<Company Name>> manager who is authorized to sign the contract);
- vendor classification;
- primary contact information;
- SLA, RTO, RPO;
- CVSS score—see the Appendix A of the Enterprise Risk Methodology;
- link to service contract; and,
- link to relevant security or privacy certifications.

3.4 ACCESS CONTROL

In some cases Service Providers require access to information or systems that are normally protected from external use. Sharing information or systems with a Service Provider is allowed, but requires the following:

- Receipt of an NDA signed by an authorized delegate of the Service Provider.
- Receipt of an MSA signed by an authorized delegate of the Service Provider.
- Submission of an “Access Control” change control request.
    - The ‘reason’ for the change control request must align with data sharing provisions stipulated in the company’s “Terms of Use” and must comply with all applicable laws and regulations.
- Approval by the CISO or an employee delegated by the CISO.

3.5 MONITORING

Service providers should be re-evaluated at least annually, or when contracts are renewed. Service Providers should be evaluated against their

- SLA performance in terms of system availability.
- SLA performance in terms of application performance—e.g. timeliness of packet requests, etc.
- Outstanding issues in terms of service tickets.
- Reputational incidents: such as data breeches, or security lapses.

3.5.1 UPTIME MONITORING

When possible, service provider systems should be monitored to ensure conformance with their stated SLA.

3.5.2 SCANNING

Periodic evaluation and scoring by a third-party to ensure that application security meets security standards.

3.6 RE-EVALUATION

Service providers should be re-evaluated at least annually, at contract renewal, or when they experience a security incident such as a data breach.

3.6.1 SYSTEM REQUIREMENTS

Each service provider should be evaluated in terms of the security requirements that they are required to adhere to. For example, a SaaS provider should be required to adhere to an SLA, RTO, and RPO. Monitoring systems should be in-place to establish compliance to standards on a periodic basis.

3.6.1.1 VENDORS THAT HOLD PROPRIETARY OR CONFIDENTIAL INFORMATION

Service providers that hold confidential data or PII must provide evidence that access to physical facilities and protected information assets is restricted to authorized personnel. <<Company Name>> should verify on a periodic basis that controls are in place to protect sensitive data. Ideally, the service provider should provide either attestation of compliance with a security standard, or proof of certification.

3.6.2 RECURRING SECURITY REQUIREMENTS AND CONTACT INFORMATION

Service providers should have the ability to update information such as contact information through a portal. They should also have the ability to upload recurring security assets such as penetration tests and certifications.

3.6.3 CVSS SCORE

The service providers CVSS score should be re-evaluated—see Appendix A of the Enterprise Risk Management Policy.

3.7 SERVICE PROVIDER OFFBOARDING

Service providers should be evaluated against a check-list of requirements to ensure that they are offboarded consistently: e.g. marking the service provider as decommissioned in the vendor catalog, archiving the vendor in the ERP system, user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

3.8 VENDOR COMMUNICATION

Changes to commitments, requirements and responsibilities, including those relating to confidentiality, are communicated to customers via updated agreements and website notices. All service providers are required to provide a method to escalate issues in the event that immediate resolution of an issue is required.

3.9 DOWNSTREAM INCIDENTS

Vendor incidents that impact <<Company Name>> should be reported to <<Company Name>> with the required breach notification window. <<Company Name>>'s incident response team to should identify the scope of the impact of the breach and report out to customers.

3.10 SOFTWARE ACCEPTANCE CRITERIA

For products and services that are built to specification for the company the following criteria should be adhered to. It should be noted, that enterprise software, e.g. software that is acquired from a reseller, or SaaS/PaaS products may not need to complete all of these steps and in some cases can be fast-tracked. The CTO is the ultimate arbiter of product acceptance criteria for the company.

3.10.1 REQUIREMENTS PRIOR TO WORK

In the event that the Service Provider is delivering a product additional criteria should be established. Namely:

1. Project management should add the project to the company's roadmap.
2. Identify a product owner who has ultimate authority to make decisions on-behalf of the company.
3. If required, identify a solution architect who can oversee technical oversight to ensure that quality standards are adhered to.
4. Evaluate an SOW with a clear agreement on the scope of work.
5. Documented security requirements.
6. Functional requirements with a formalized User Acceptance Testing (UAT) plan. The UAT plan must be reviewed and approved by the product owner.
7. Non-functional requirements—such as performance thresholds and error budgets. This documentation should also include architectural diagrams, service boundary descriptions, and dataflow documentation such as sequence diagrams. The CTO must sign-off on non-functional requirements prior to the start of work.
8. If applicable, project management should have read access to the service providers backlog and Kanban board.
9. If required, create a project plan for deployment.
10. If required, ensure that a support agreement and support documentation is negotiated.

3.10.2 REQUIREMENTS ON DELIVERY

The product must satisfy the following criteria prior to deployment:

1. Successful completion of non-functional requirements, e.g. load-testing, etc.
2. Successful completion of security requirements: penetration testing, DAST, SAST, etc.
3. Successful completion of functional requirements, e.g. completion of UAT and sign-off from the product owner.
4. Validation of delivery against SOW—e.g. that all agreed upon deliverables where completed.

If all the acceptance criteria is satisfactory the product owner should create a change control ticket to signal the deployment has been approved for deployment.

3.11 ISSUE REPORTING

Service providers can report and track system issues or make an anonymous complaint.

4 REVIEW

Executive management meets at least annually with operational management to review vendor management policy.

5 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

6 DOCUMENT RACI

Responsible	Assigned to do the work	Security Program Manager
Accountable	Final decision, ultimately answerable	ISM Governance Committee
Consulted	Consulted BEFORE an action or decision is taken (proactive)	Executive Management
Informed	Informed AFTER a decision or action has been taken (reactive)	Named Participants in this document Other parties affected by the change

7 LICENSE INFORMATION

8 APPENDIX A: VENDOR CONTRACT PROVISIONS

<<Company Name>> uses the Common Vulnerability Scoring System (CVSS) methodology to assess and assign contract provisions for Service Providers.

CVSS Score	Right to Audit	Background Check	BC/DR	Confidentiality	Consumer Complaints	Equal Opportunity	Insurance	SLA
Critical	X	X	X	X	X	X	X	X
High	X	X	X	X	X	X	X	X
Medium	X	X	X			X	X	
Low						X		
None								