stereopsia EUROPE

Third Party Risk Management Policy

1. Purpose and Scope

This Third Party Risk Management Policy outlines the procedures and guidelines for assessing, mitigating, and monitoring risks associated with engaging third-party partners, and service providers. The policy is designed to ensure that Stereopsia's operations, data, and reputation are protected while conducting business with external entities.

2. Third Party Identification and Selection

- Prior to engaging with a third party, a comprehensive assessment should be conducted to determine the necessity of the engagement and the potential risks involved.
- Third parties must undergo a due diligence process that evaluates their financial stability, reputation, compliance with relevant regulations, and security practices.

3. Risk Assessment and Classification

- Third parties should be classified based on the potential impact they could have on the organization's operations, data, and reputation.
- Risk assessments should consider factors such as the type of services provided, access to sensitive data, and the third party's security controls.

4. Contractual Agreements

- Written agreements should be established with third parties, clearly outlining the terms and conditions of the engagement.
- Contracts should include clauses related to data protection, confidentiality, security requirements, compliance with laws, and incident response procedures.

5. Security and Privacy Requirements

- Third parties should adhere to the organization's security and privacy standards and controls.
- Security assessments may be required to ensure third parties meet established security criteria.

6. Ongoing Monitoring and Due Diligence

- Regular monitoring of third party activities is essential to identify any changes in their risk profile.
- Periodic assessments should be conducted to ensure third parties continue to meet the organization's security and compliance expectations.

7. Incident Management and Reporting

- Third parties must promptly report any security incidents or breaches to the organization.
- The organization and third party should collaborate on incident response and mitigation.

8. Exit Strategy

- An exit strategy should be defined in case the engagement with a third party needs to be terminated.
- This strategy should include steps for retrieving data, transitioning services, and ensuring a smooth transition.

9. Review and Improvement

- This policy should be periodically reviewed and updated to ensure it aligns with changing business requirements and the evolving risk landscape.

10. Training and Awareness

- Employees involved in engaging and managing third parties should receive training on this policy and associated procedures.

Conclusion

The Third Party Risk Management Policy ensures that third-party engagements are conducted with a comprehensive understanding of associated risks. By following the procedures outlined in this policy, the organization aims to safeguard its operations, data, and reputation while maintaining strong relationships with external partners.