Service Definition Document:

Cybersecurity Services

1. Service Overview:

Our Cybersecurity Services offer comprehensive solutions designed to protect organizations from cyber threats and safeguard their digital assets, infrastructure, and sensitive information. Leveraging industry-leading technologies, expert knowledge, and best practices, we specialize in identifying vulnerabilities, mitigating risks, and enhancing security posture to ensure resilience against cyber attacks.

2. Data Backup, Restore, and Disaster Recovery:

While our Cybersecurity Services do not directly involve data backup and restore, we prioritize data security and integrity throughout our engagements. We assist clients in developing business continuity and disaster recovery plans to ensure operational resilience in the event of unforeseen incidents.

3. Onboarding and Offboarding Support:

We provide comprehensive onboarding support to help clients seamlessly integrate our Cybersecurity Services into their operations. Similarly, offboarding support is offered to ensure a smooth transition and knowledge transfer upon termination of services.

4. Service Constraints:

Service constraints may include maintenance windows, during which temporary disruptions to service availability may occur. The level of customization allowed is determined based on

project scope and requirements, balancing flexibility with project deadlines and budget constraints.

5. Service Levels:

Our service levels prioritize performance, availability, and support responsiveness. We commit to meeting or exceeding agreed-upon performance benchmarks, ensuring high availability of security resources, and providing timely support during specified hours.

6. After Sales Support:

We offer ongoing after-sales support to address post-implementation needs, including troubleshooting, optimization, and guidance on leveraging cybersecurity solutions effectively to achieve business objectives. Support channels may include email, phone, or dedicated support portals.

7. Technical Requirements:

Technical requirements for our Cybersecurity Services may vary based on project scope and objectives. However, clients are generally expected to provide access to relevant systems, networks, and security infrastructure to facilitate collaboration and implementation.

8. Outage and Maintenance Management:

We proactively manage outages and scheduled maintenance activities to minimize disruption to service. Clients are notified in advance of any planned maintenance windows, and efforts are made to ensure minimal impact on security operations and incident response capabilities.

9. Hosting Options and Locations:

Our Cybersecurity Services do not involve hosting infrastructure. However, we can provide guidance on hosting options and locations based on client requirements and preferences, including cloud-based solutions and third-party hosting providers.

10. Access to Data (Upon Exit):

- Upon termination of services, clients retain full ownership and access to their data and security assets. We facilitate data extraction and provide assistance with transitioning to alternative service providers as needed, ensuring a seamless exit process.

11. Security:

- Security is paramount in our service delivery. We adhere to industry best practices and standards to ensure the confidentiality, integrity, and availability of client data throughout the engagement. Measures include encryption, access controls, and adherence to data protection regulations.

This Service Definition Document outlines the key aspects of our Cybersecurity Services. We are committed to delivering high-quality, innovative security solutions that empower organizations to protect their assets, mitigate risks, and maintain a resilient security posture in today's evolving threat landscape.