**Annex 2 - Security Measures**

This Annex forms part of the DPA.

Defradar currently observes the Security Measures described in this Annex 2. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

**a) Access Control**

i)  Preventing Unauthorized Product Access

**Outsourced processing:** Defradar hosts its Service with outsourced cloud infrastructure providers. Additionally, Defradar maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement. Defradar relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect  data processed or stored by these vendors.

**Physical and environmental security:** Defradar hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: Defradar implemented a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

**Authorization:** Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Defradar’s products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user’s permissions against the attributes associated with each data set.

**Application Programming Interface (API) access:** Public product APIs may be accessed using an API key or through Oauth authorization.

ii)  Preventing Unauthorized Product Use

Defradar implements industry standard access controls and detection capabilities for the internal networks that support its products.

**Access controls:** Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure  providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: Defradar implemented a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

**Static code analysis:** Security reviews of code stored in Defradar’s source code repositories is performed, checking for coding best practices and identifiable software flaws.

**Penetration testing:** Defradar maintains relationships with industry recognized penetration testing service providers for four annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

**Bug bounty:** A bug bounty program invites and incentivizes independent security researchers to ethically discover and disclose security flaws. Defradar implemented a bug bounty program in an effort to widen the available opportunities to engage with the security community and improve the product defenses against sophisticated attacks.

iii)    Limitations of Privilege & Authorization Requirements

**Product access:** A subset of Defradar’s employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through “just in time” requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

**Background checks:** All Defradar employees undergo a third-party background check prior to being extended an employment offer, in accordance with and as permitted by the applicable laws. All employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

**b) Transmission Control**

**In-transit:** Defradar makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer site hosted on the Defradar products. Defradar’s HTTPS implementation uses industry standard algorithms and certificates.

**At-rest:** Defradar stores user passwords following policies that follow industry standard practices for security.  Defradar has implemented technologies to ensure that stored data is encrypted at rest.

**c) Input Control**

**Detection:** Defradar designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Defradar personnel, including security, operations, and support personnel, are responsive to known incidents.

**Response and tracking:** Defradar maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, Defradar will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to Customer will be in accordance with the terms of the DPA or Agreement.

**d) Availability Control**

**Infrastructure availability:** The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

**Fault tolerance:** Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

**Online replicas and backups:** Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

Defradar’s products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists Defradar operations in maintaining and updating the product applications and backend while limiting downtime.