



Service Document for Security Services v3.3



Version History		
Version Number	Date Approved	Change/Reason for Change/Comments
2.2	23/08/2023	Initial document creation. Aligns to Exponential-e Security Service portfolio July 2023 and Exponential-e Service Document v2.2. Version number is to align to Exponential-e version control – no earlier Vysiion version exists.
2.3	03/05/2024	Addition of Forticlient EMS Service, Security Awareness Training and Managed Email Security
3.0	02/05/2025	Removal of data processing provisions. Changes to inflationary price increase provisions.
3.1	16/10/2025	Removal of reference to Windows server required for FortiClient EMS Service. Addition of Microsoft Sentinel Cyber Security Operations Centre Service. Removal of Secured Managed Firewall Service, Advanced Firewall Monitoring, Next Generation Unified Threat Management Service, and Next Generation Firewall Service. Addition of Dedicated Firewall and Centralised Firewall Services.
3.2	13/03/2026	Addition of Decommissioning Costs into the main body.
3.3	07/09/2026	Patching clause inserted into the main body; addition of planned and/or emergency works as an Excused Reason; minor amendment to the Target Service Commencement Date for Cyber Security Operations Centre Service; Managed Email Security amended to include licence bundle options; and addition of FortiSASE TM Service.

1. Document Purpose

This document describes Vysiion's security services, their service level agreements (if applicable) and the service-specific terms and conditions that are applicable, in addition to Vysiion's General Terms. Capitalised terms used in this Service Document which are defined in the General Terms shall be afforded their defined meanings throughout this Service Document.

2. Security Services Portfolio

Each Security Service is set out in a separate Service Definition attached as a schedule.

3. Service Delivery and Acceptance

Vysiion will liaise with the Customer to ensure that all relevant information is obtained and provide regular progress reporting and on-going support during delivery. All activities related to delivery are scheduled within Normal Business Hours. If the Parties agree to re-schedule these outside of Normal Business Hours additional charges shall apply. Vysiion will notify the Customer by email when the Service(s) is ready to be used. Where applicable to a Service, acceptance tests are set out in the relevant Service Definition.

4. Service Support

4.1 Fault Management

Information on how to contact Vysiion's Service Desk and fault reporting can be found in the "Customer Support Handbook", a copy of which is available upon request from Vysiion.

4.2 Service Moves

Vysiion will, if it is technically possible to move the Services from a current Customer Site to a new Customer Site, provide a quotation to the Customer.

4.3 Planned and Emergency Works

Vysiion will aim to provide at least 10 days' notice via email of any planned works. Vysiion reserves the right to carry out emergency works at any time, without notice.

5. Service Commencement Dates

Unless otherwise specified in the Contract, the Service Commencement Date for a Service at a Site is the earlier of (i) the date on which the Service is handed over and (ii) when the Customer begins to use the Service. For centralised services shared by multiple Sites (i.e. Centralised Firewall etc.) the Service Commencement Date is the date on which that Service has been handed over and is accessible from at least one (1) Site.

6. Service Credits

6.1 Service Availability

The target availability for each Security Service (if applicable) is provided in the relevant Service Definition. Unless set out otherwise in the applicable Service Definition, the Availability is calculated on a calendar monthly basis using a 730 hour month and the following formula:

$$P = \frac{730 \text{ Hours} - A}{730 \text{ Hours}} \times 100$$

Where P = Percentage availability; A = Sum of all events of unavailable service in that month measured in hours. Non-availability is measured from the time an incident ticket is raised to the time the service is restored and the incident ticket is cleared by Vysiion.

6.2 Service Credit Rules

Vysiion shall have no liability for any failure to meet any target service levels due to, or as a result of, any of the following reasons ("Excused Reasons"):

- Non-availability of Vysiion connectivity services (including any CPE) – only the service level agreement for the connectivity service shall apply;
- Non-availability of internet access or non-availability due to cyber-attack;
- The use of the Service for a purpose for which it was not designed or specified for;
- The diagnosis and correction of any fault in equipment for which Vysiion is not providing support services;
- Any Force Majeure Event;
- Suspension of service in accordance with the Contract;

- Customer default or delay, or any negligent, wilful or reckless act, fault or omission by the Customer or any users for whom the Customer is responsible under the Contract, or any of their representatives, employees, agents or sub-contractors;
- Access issues and delays along the route of the Service(s) or at the Customer Site(s);
- Third party software including but not limited to software bugs and/or Malicious Code; and/or
- Planned and/or emergency works.

6.3 How to Claim

Service credit claims must be submitted to customerservices@vysiion.co.uk within thirty (30) calendar days of the end of the calendar month in which the failure to meet the target service level has occurred. Any service credit claims not raised within this period are irrevocably waived. If service credits claimed are rightly due, they shall be calculated in accordance with the relevant Service Definition and this section (such service credits being a genuine pre-estimate of loss, not unconscionable and not a penalty) and be applied to the Customer's account. Service credits shall be the Customer's sole and exclusive remedy with respect to any failure to meet target service levels. Monthly Charges referred to in this Service Document are to the Annual Charges divided by twelve (12).

7. Complaints

Details of Vysiion's complaints process and policy are available upon request from customerservices@vysiion.co.uk.

8. Additional Terms

8.1 CHARGES

8.1.1 Vysiion shall be entitled to increase the Annual Charges:

8.1.1.1 in line with any increases in costs as a result of legal and/or regulatory changes; and/or

8.1.1.2 in line with inflation (where any such increase shall be limited to the change in the UK Retail Price Index (or any materially-equivalent replacement index) plus two percent (2%) since signature of the Contract (in the case of the first such inflationary increase) or since any previous inflationary increase (in the case of any subsequent inflationary increases); and/or

8.1.1.3 in line with any increases in costs imposed upon Vysiion by its suppliers.

Vysiion will provide reasonable documentary evidence to support such price increase to the Customer, upon request.

8.1.2 If the Contract involves the purchase by Vysiion of goods and/or services in a currency other than sterling and there is a greater than one percent (1%) change in the exchange rate between sterling and that other currency due to the weakening of sterling between (a) the date of Order acceptance and (b) the date that Vysiion pays the relevant supplier, Vysiion reserves the right to pass on to the Customer the additional costs incurred by Vysiion as a result of the change in exchange rates and the Customer agrees to pay the same.

8.2 Decommissioning Costs

Upon termination or expiry of the Contract (or an element thereof), Vysiion shall be entitled to invoice the Customer for Decommissioning Costs.

8.2 SOFTWARE

8.2.1 The following Patch management policy shall apply in respect of the Service(s). Software/Firmware patches shall be applied when deemed necessary by the Vysiion Operational Centre. Patching could be triggered under various conditions:

8.2.1.1 A remotely exploitable security vulnerability is identified and the vendor releases a patch for the vulnerability. Vysiion software release management function conducts a regular review of new vulnerabilities and assesses the functional and security risk to platforms under its remit. It is often the case that vulnerabilities are only applicable if certain configuration is present on the device in question, and if certain features are enabled. If the net effect is that no vulnerability is exposed, then the patch would not be applied. If vulnerability is exploitable but it is feasible to amend configuration in such a

way as to prevent the vulnerability being exploited, then the patch would also not be applied – however in this case the work-around configuration would be introduced under the normal change control procedures;

- 8.2.1.2 A normal end of lifecycle upgrade may be triggered when vendor support of the technology in question is no longer available. In certain circumstances a hardware refresh or upgrade would be required, which falls outside the scope of this patch management policy;
- 8.2.1.3 A bug is identified which is adversely affecting the reliable operation of the device. It is frequently the case that bugs are triggered only under certain specific conditions which are not present in all environments. Under these circumstances Vysiion will assess whether the bug potentially has widespread impact (in which case the patch would be rolled out to all similar devices under Vysiion management), or the condition is isolated (in which case only the particular affected device would be patched).
- 8.2.2 Patch Management excludes security hardening required for regulatory or compliance purposes. This will be a chargeable Professional Services engagement.
- 8.2.3 The following Release management policy shall apply in respect of the Service(s). Only software updates relating to the operating system supported by the vendor shall be implemented by the Vysiion Operational Centre. Software is managed within the following guidelines:
- 8.2.3.1 Vendor announcements and vulnerability announcements are continually reviewed by Vysiion in order to identify new software vulnerabilities;
- 8.2.3.2 In case a vendor announces a new remotely exploitable vulnerability and releases a patch to address the vulnerability for which no workaround exists, an upgrade will be initiated by Vysiion. In many cases a particular vulnerability requires a specific configuration to be present. Vysiion will analyse the impact of the vulnerability on Vysiion managed devices, as covered by the Contract, and propose either an upgrade or a workaround if the vulnerability is remotely exploitable;
- 8.2.3.3 A release of software becomes end of support due to the end of lifecycle as determined by the vendor;
- 8.2.3.4 A specific bug is identified that impacts the Customer environment in terms of performance or stability of the platform.
- 8.2.3.5 The Customer may request an upgrade to a version of the operating system software fully supported by Vysiion as part of the Service through a service request.
If none of the above scenarios are met, Vysiion will not proceed to release a new software revision.
- 8.2.3.6 Vysiion shall use reasonable efforts to assess, test, and deploy patches, hotfixes, or other mitigations addressing newly released security vulnerabilities for in-scope managed systems, in accordance with the following target remediation timeframes, measured from the date on which a patch, hotfix, or workaround by the applicable software vendor is made available:
- Critical vulnerabilities: within fourteen (14) calendar days
 - High vulnerabilities: within thirty (30) calendar days
- Vulnerability severity shall be determined based on vendor classification or, where not specified, an industry-standard scoring system such as CVSS.
- Where a software vendor or third party has not yet released an applicable patch, hotfix, or workaround, or where Vysiion reasonably determines that deployment within the target timeframe would introduce unacceptable operational or security risks (including change restrictions or approval dependencies), Vysiion shall implement appropriate interim risk mitigation measures and continue to monitor for, and apply, the relevant updates as soon as reasonably practicable thereafter.
- 8.2.4 VYSIION SHALL HAVE NO LIABILITY FOR ANY SECURITY INCIDENTS OR SERVICE FAULTS/ERRORS/FAILURES TO THE EXTENT DUE TO THIRD PARTY SOFTWARE.