SonicWall - Data Processing Agreement

This Data Processing Agreement ("**DPA**") governs SonicWall's processing of your personal data when it provides products and/or services to you.

1. *Definitions:* In this DPA, the following terms shall have the following meanings:

   (a) "**controller**", "**processor**", "**data subject**", "**personal data**" and "**processing**" (and "**process**") shall have the meanings given in EU/UK Data Protection Law;

   (b) "**Agreement**" means the agreement(s) between Customer and SonicWall under which SonicWall agrees to provide certain products and/or services to Customer;

   (c) "**Applicable Data Protection Law**" means all worldwide data protection and privacy laws and regulations applicable to the personal data in question, including, where applicable, EU/UK Data Protection Law;

   (d) "**Customer**" or "**you**" means the party that engages SonicWall to provide products and/or services under the Agreement;

   (e) "**EEA**" means the European Economic Area;

   (f) "**EU/UK Data Protection Law**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**"); (ii) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (iii) the EU e-Privacy Directive (Directive 2002/58/EC); and (iv) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (i), (ii) or (iii); in each case as may be amended or superseded from time to time;

   (g) "**Restricted Transfer**" means: (i) where the EU GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; and (ii) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject to adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018;

   (h) "**SonicWall**" means SonicWall Inc. or any affiliated entity of SonicWall Inc. that provides products and/or services to you under an Agreement; and

   (i) "**Standard Contractual Clauses**" means: (i) where the EU GDPR applies, the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, the "International Data Transfer Addendum to the EU Commission

Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**").

2. *Relationship of the parties:* Customer (the controller) appoints SonicWall as a processor to process the personal data that is described in Annex I of this DPA (the "**Data**"). Each party shall comply with the obligations that apply to it under Applicable Data Protection Law in connection with its processing of the Data.

3. *Purpose limitation:* SonicWall shall process the Data as a processor strictly in accordance with the documented instructions of Customer (the "**Permitted Purpose**"), except where otherwise required by law(s) that are not incompatible with Applicable Data Protection Law. For the purposes of this DPA, the Permitted Purpose is to process the Data (i) as necessary to perform its obligations under the Agreement; (ii) as necessary to comply with applicable laws; and (iii) in accordance with any other instructions documented in this DPA by the Parties from time to time. SonicWall shall immediately inform Customer if it becomes aware that Customer's processing instructions infringe Applicable Data Protection Law (but without obligation to actively monitor Customer's compliance with Applicable Data Protection Law).

4. *Restricted transfers:* The parties agree that when the transfer of Data from Customer to SonicWall is a Restricted Transfer it shall be subject to the appropriate Standard Contractual Clauses as follows:

   (a) in relation to Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

      (i) Module Two will apply;

      (ii) in Clause 7, the optional docking clause will apply;

      (iii) in Clause 9, Option 2 will apply, and the time period for prior notice of subprocessor changes shall be as set out in Clause 9 of this DPA;

      (iv) in Clause 11, the optional language will not apply;

      (v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by Irish law;

      (vi) in Clause 18(b), disputes shall be resolved before the courts of Ireland;

      (vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex II to this DPA; and

      (viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex III to this DPA;

   (b) in relation to Data that is protected by the UK GDPR, the UK Addendum will apply completed as follows:

(i) The EU SCCs, completed as set out above in clause 4(a) of this DPA shall also apply to transfers of such Data, subject to sub-clause (ii) below;

(ii) Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the EU SCCs, completed as set out above, and the options "neither party" shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this DPA.

(c) in the event that any provision of this DPA contradicts, directly or indirectly, the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

5. *Onward transfers:* SonicWall shall not participate in (nor permit any subprocessor to participate in) any other Restricted Transfers of Data (whether as an exporter or an importer of the Data) unless the Restricted Transfer is made in full compliance with Applicable Data Protection Law and pursuant to Standard Contractual Clauses implemented between the exporter and importer of the Data.

6. *Confidentiality of processing:* SonicWall shall ensure that any person that it authorises to process the Data (including SonicWall's staff, agents and subprocessors) (an "**Authorised Person**") shall be subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty), and shall not permit any person to process the Data who is not under such a duty of confidentiality.

7. *Security:* SonicWall shall implement appropriate technical and organisational measures to protect the Data from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure or access (a "**Security Incident**").

8. *Security incidents:* Upon becoming aware of a Security Incident, SonicWall shall inform Customer without undue delay and shall provide all such timely information and cooperation as Customer may require in order for Customer to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. SonicWall shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the Security Incident and shall keep Customer informed of all developments in connection with the Security Incident.

9. *Subprocessing:* The Customer authorises SonicWall to engage third party subprocessors to process the Data provided that:

(a) SonicWall provides at least 30 days' prior notice of the addition or removal of any subprocessor (including details of the processing it performs or will perform), which may be given by posting details of such addition or removal at the following URL: https://www.sonicwall.com/legal/sub-processors/;

(b) SonicWall imposes data protection terms on any subprocessor it appoints that protect the Data, in substance, to the same standard provided for by this Clause; and

(c) SonicWall remains fully liable for any breach of this Clause that is caused by an act, error or omission of its subprocessor.

If Customer objects to the addition or removal of any subprocessor on reasonable grounds relating to the protection of the Data, then either SonicWall will not appoint the subprocessor or Customer may elect to suspend or terminate the Agreement (but without prejudice to Customer's obligation to pay any fees or other charges under the Agreement for products and/or services provided to Customer on or before the date of such suspension or termination).

10. *Cooperation and data subjects' rights:* SonicWall shall provide all reasonable and timely assistance to Customer (at Customer's expense) to enable Customer to respond to:

(a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and

(b) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Data,

and, in the event that any such request, correspondence, enquiry or complaint is made directly to SonicWall, SonicWall shall promptly inform Customer providing full details of the same.

11. *Data Protection Impact Assessment:* SonicWall shall provide Customer with all such reasonable and timely assistance as Customer may require in order to conduct a data protection impact assessment in accordance with Applicable Data Protection Law including, if necessary, to assist Customer to consult with its relevant data protection authority.

12. *Deletion or return of Data:* Upon termination or expiry of the Agreement, SonicWall shall (at Customer's election) destroy or return to Customer all Data (including all copies of the Data) in its possession or control (including any Data subcontracted to a third party for processing). This requirement shall not apply to the extent that SonicWall is required by any applicable law to retain some or all of the Data, in which event SonicWall shall isolate and protect the Data from any further processing except to the extent required by such law until deletion is possible.

13. *Audit:* SonicWall shall permit Customer (or its appointed third party auditors) to audit SonicWall's compliance with its obligations under EU GDPR and UK GDPR Article 28, and shall make available to Customer all information, systems and staff necessary for Customer (or its third party auditors) to conduct such audit. SonicWall acknowledges that Customer (or its third party auditors) may enter its premises for the purposes of conducting this audit, provided that Customer gives it reasonable prior notice of its intention to audit, conducts its audit during normal business hours, takes all reasonable measures to prevent unnecessary disruption to SonicWall's operations and pays for SonicWall's reasonable costs for assisting with the provision of such information, and access to such systems and staff and for allowing for and contributing to such audits. Customer will not exercise its audit

rights more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority; or (ii) Customer reasonably believes a further audit is necessary due to a Security Incident suffered by SonicWall.

Execution

Signed for and on behalf of **SonicWall Inc.** By:_____ Printed Name:_____ Title:_____ Date:_____	Signed for and on behalf of **Customer** Company:_____ By:_____ Printed Name:_____ Title:_____ Date:_____ Notification Address:_____ Notification E-mail:_____

Please print this document, provide the information requested, and have the DPA signed by an authorised representative of the Customer. Send a copy of the executed DPA to dataprivacy@sonicwall.com. SonicWall will then execute the DPA and return a copy to the email address provided in the signature line.

Annex I

Data Processing Description

Subject matter of processing	SonicWall will process Data as necessary to provide the products and/or services under the Agreement and as further specified in any documentation associated with the products and/or services.
Duration of processing	The duration of the processing will be until the earliest of (i) expiration or termination of the Agreement; or (ii) the date upon which such processing is no longer necessary to achieve the purpose of processing. The provisions of this DPA shall apply for as long as your Data is in SonicWall's possession and/or control.
Nature and purpose of processing	The objective of the processing of Data by SonicWall Inc. is to provide the products and/or service, pursuant to the Agreement.
Type of Data	Data includes data as defined in the Agreement, the DPA, or as otherwise specified herein.
Categories of data subjects	Categories of Subjects includes Data Subjects as defined in the DPA including but not limited to end users of the Customer.

Annex II

Data Transfer Description

This Annex II forms part of the Agreement and describes the processing that the processor will perform on behalf of the controller.

A. LIST OF PARTIES

Controller(s) / Data exporter(s): [*Identity and contact details of the controller(s) /data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

1.	Name:	See details provided in the execution block above
	Address:	See details provided in the Agreement for the party identified in the execution block above
	Contact person's name, position and contact details:	See details provided in the execution block above
	Activities relevant to the data transferred under these Clauses:	The engagement of SonicWall to provide certain products and/or services as set out under the Agreement
	Signature and date:	See execution block above
	Role (controller/processor):	Controller

Processor(s) / Data importer(s): *[Identity and contact details of the processor(s) /data importer(s), including any contact person with responsibility for data protection*]

1.	Name:	The SonicWall entity identified in the signature block above.
	Address:	See details provided in the Agreement for the party identified in the execution block above
	Contact person's name, position and contact details:	Chief Privacy Officer at dataprivacy@sonicwall.com
	Activities relevant to the data transferred under these Clauses:	The provision of products and/or services to Customer as set out in the Agreement
	Signature and date:	See execution block above
	Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	As set out in Annex I "Categories of data subjects"
Categories of personal data transferred:	As set out in Annex I "Types of personal data"
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose	SonicWall does not have access to, process or store a Customer's data via SonicWall's firewall hardware appliances without a subscription to the SonicWall Capture Advanced Threat

limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	Protection sandbox service. The personal data, if any, would be limited to any actual or live data that may be included in the Customer's email leveraged by a threat actor. SonicWall Capture Cloud Platform and SonicWall's Cloud Edge Secure Access enables Customer's designated end-user personnel to access their network data in an environment hosted by SonicWall. SonicWall does not access, store or otherwise process the data.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Continuous
Nature of the processing:	As set out in Annex I "Nature and purpose of processing"
Purpose(s) of the data transfer and further processing:	As set out in Annex I "Nature and purpose of processing"
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	As set out in Annex I "Duration of processing"
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	N/A

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	The supervisory authority selected by virtue of clause 13 of the Standard Contractual Clauses

Annex III

Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by SonicWall (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

SonicWall takes information security seriously and this approach is followed through in its processing and transfers of Data. This information security overview applies to SonicWall's corporate controls for safeguarding Data which is processed and transferred amongst the SonicWall group companies. SonicWall's information security program enables the workforce to understand their responsibilities.

SECURITY PRACTICES

SonicWall has implemented corporate information security practices and standards that are designed to safeguard SonicWall's corporate environment and to address business objectives across the following areas: (1) information security, (2) system and asset management, (3) development, and (4) governance. These practices and standards are approved by the SonicWall management and are periodically reviewed and updated where necessary. SonicWall shall maintain an appropriate data privacy and information security program, including policies and procedures for physical and logical access restrictions, data classification, access rights, credentialing programs, record retention, data privacy, information security and the treatment of Data throughout its lifecycle.

ORGANISATIONAL SECURITY

It is the responsibility of the individuals across the SonicWall organisation to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, SonicWall's Information Security ("**IS**") function is responsible for the following activities:

1. Security strategy – the IS function drives SonicWall's security direction. The IS function works to ensure compliance with security related policies, standards and regulations, and to raise awareness and provide education to users. The IS function also carries out risk assessments and risk management activities and manages contract security requirements.
2. Security engineering – the IS function manages testing, design and implementation of security solutions to enable adoption of security controls across the environment.
3. Security operations – the IS function manages support of implemented security solutions, monitors and scans the environment and assets, and manages incident response.
4. Forensic investigations – the IS function works with Legal, and Human Resources to carry out investigations, including eDiscovery and eForensics.
5. Security consulting and testing – the IS function works with software developers on developing security best practices, consults on application development and architecture for software projects, and carries out assurance testing.

ASSET CLASSIFICATION AND CONTROL. SonicWall's practice is to track and manage key information and physical, software and logical assets. Examples of the assets that SonicWall might track include:

1. Information assets, such as identified databases, Data classification, archived information.
2. Software assets, such as identified applications and system software.
3. Physical assets, such as identified servers, desktops/laptops, backup/archival tapes, printers and communications equipment.

EMPLOYEE SCREENING, TRAINING AND SECURITY

1. Screening/background checks: Where reasonably practicable and appropriate, as part of the employment/recruitment process, SonicWall shall perform screening/background checks on employees (which shall vary from country to country based on local laws and regulations), where such employees will have access to SonicWall's networks, systems or facilities.
2. Identification: SonicWall shall require all employees to provide proof of identification and any additional documentation that may be required based on the country of hire or if required by other SonicWall entities or customers for whom the employee is providing services.
3. Training: SonicWall's annual compliance training program includes a requirement for employees to complete a Data protection and information security awareness course and pass an assessment at the end of the course. The security awareness course may also provide materials specific to certain job functions.
4. Confidentiality: SonicWall shall ensure its employees are legally bound to protect and maintain the confidentiality of any Data they handle pursuant to standard agreements.

PHYSICAL ACCESS CONTROLS AND ENVIRONMENTAL SECURITY

1. Physical security program: SonicWall shall use appropriate safeguards in its physical security program to mitigate security risks to the extent reasonably practicable.
2. Physical access controls: Physical access controls/security measures at SonicWall's facilities/premises are designed to meet the following requirements:
   (a) access to SonicWall's buildings, facilities and other physical premises shall be controlled and based upon business necessity, sensitivity of assets and the individual's role and relationship to SonicWall. Only personnel associated with SonicWall are provided access to SonicWall's facilities and physical resources in a manner consistent with their role and responsibilities in the organization;
   (b) relevant SonicWall facilities are secured by an access control system;
   (c) all persons requiring access to facilities and/or resources are issued with appropriate and unique physical access credentials (e.g. a badge or keycard assigned to one individual) by the IS function. Individuals issued with unique physical access credentials are instructed not to allow or enable other individuals to access SonicWall facilities or resources using their unique credentials (e.g. no "tailgating"). Temporary credentials may be issued to individuals who do not have active identities where this is necessary (i) for access to a specific facility and (ii) for valid business needs. Unique credentials are non-transferable and if an individual cannot produce their credentials upon request they may be denied entry to SonicWall's facilities or escorted off the premises. At staffed entrances, individuals are required to present a valid photo identification or valid credentials to the security representative upon entering. Individuals who have lost or misplaced their credentials or other identification are required to enter through a staffed entrance and be issued a temporary badge by a security representative;
   (d) SonicWall's employees are trained to always carry their credentials, store their laptops, portable devices and documents in a secure location (especially while traveling) and log out or shut down their computers when away from their desk;
   (e) visitors who require access to SonicWall facilities must enter through a staffed and/or main facility entrance. To prevent access to, or disclosure of, company proprietary information visitors are not allowed un-escorted access to restricted or controlled areas;
   (f) select SonicWall facilities use CCTV monitoring, security guards and other physical measures where appropriate and legally permitted;
   (g) locked shred bins are provided on most sites to enable secure destruction of confidential information and Data;
   (h) for software development and infrastructure deployment projects, the IS function uses a risk evaluation process and a Data classification program to manage risk arising from such activities.

CHANGE MANAGEMENT. The IT organisation manages changes to the corporate infrastructure, systems and applications through a centralized change management program, which may include testing, business impact analysis and management approval where appropriate. All relevant application and systems developments adhere to an approved change management process.

SECURITY INCIDENTS AND RESPONSE PLAN

1. Security incident response plan: SonicWall maintains a security incident response policy and related plan and procedures which address the measures that SonicWall will take in the event of loss of control, theft, unauthorised disclosure, unauthorized access, or unauthorised acquisition of Data. These measures may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

2. Response controls: Controls are in place to protect against, and support the detection of, malicious use of assets and malicious software and to report potential incidents to SonicWall's' IS function or Service Desk for appropriate action. Controls may include, but are not limited to: information security policies and standards; restricted access; designated development and test environments; virus detection on servers, desktop and notebooks; virus email attachment scanning; system compliance scans; intrusion prevention monitoring and response; firewall rules; logging and alerting on key events; information handling procedures based on data type; e-commerce application and network security; and system and application vulnerability scanning. Additional controls may be implemented based on risk.

DATA TRANSMISSION CONTROL AND ENCRYPTION. SonicWall shall, to the extent it has control over any electronic transmission or transfer of Data, take all reasonable steps to ensure that such transmission or transfer cannot be read, copied, altered or removed without proper authority during its transmission or transfer. SonicWall will:

1. Implement industry-standard encryption practices in its transmission of Data. Industry-standard encryption methods used by SonicWall includes Secure Sockets Layer (SSL), Transport Layer Security (TLS), a secure shell program such as SSH, and/or Internet Protocol Security (IPSec);
2. If technically feasible, encrypt Data when transmitting or transferring that Data over any public network, or over any network not owned and maintained by SonicWall. SonicWall's policy recognises that encryption is ineffective unless the encryption key is inaccessible to unauthorised individuals and instructs personnel never to provide an encryption key via the same channel as the encrypted document; and
3. For internet-facing applications that may handle sensitive Data and/or provide real-time integration with systems on a network that contains such information (including SonicWall's core network), a Web Application Firewall (WAF) may be used to provide an additional layer of input checking and attack mitigation. The WAF will be configured to mitigate potential vulnerabilities such as injection attacks, buffer overflows, cookie manipulation and other common attack methods.

SYSTEM ACCESS CONTROLS. Access to SonicWall's systems is restricted to authorised users. Access is granted based on formal procedures designed to ensure appropriate approvals are granted to prevent access from unauthorised individuals. Such procedures include:

1. admission controls (i.e. measures to prevent unauthorised persons from using Data processing systems):
   (a) access is provided based on segregation of duties and least privileges to reduce the risk of misuse, intention or otherwise;
   (b) access to IT systems will be granted only when a user is registered under a valid username and password;

(c) SonicWall has a password policy in place which requires strong passwords for user login to issued laptops, prohibits the sharing of passwords, prohibits the use of passwords that are also used for non-work functions, and advises users on what to do in the event their password or other login credentials are lost, stolen or compromised;
(d) mandatory password changes on a regular basis;
(e) automatic computer lock, renewed access to the PC only after new registration with a valid username and password;
(f) Data and user classification determines the type of authentication that must be used by each system; and
(g) remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place as well as user authentication.

2. access controls (i.e. measures to prevent unauthorised access to systems):
   (a) access authorisation is issued in respect of the specific area of work the individual is assigned to (i.e. work role);
   (b) adjustment of access authorisations in case of changes to the working area, or in case an employee's employment is terminated for any reason;
   (c) granting, removing and reviewing administrator privileges with the appropriate additional controls and only as needed to support the system(s) in question; and
   (d) event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

DATA ACCESS CONTROL. SonicWall applies the controls set out below regarding the access and use of Data:

1. personnel are instructed to only use the minimum amount of Data necessary to achieve SonicWall's relevant business purposes;
2. personnel are instructed not to read, copy, modify or remove Data unless necessary to carry out their work duties, and;
3. third party use of Data is governed through contractual terms and conditions between the third party and SonicWall which impose limits on the third party's use of Data and restricts such use to what is necessary for the third party to provide services.

SEPARATION CONTROL. Where legally required, SonicWall will ensure that Data collected for different purposes can be processed separately. SonicWall shall also ensure there is separation between test and production systems.

AVAILABILITY CONTROL. SonicWall protects Data against accidental destruction or loss by following these controls:

1. Data is retained in accordance with this DPA or SonicWall's record management policy and practices, as well as legal retention requirements;
2. hardcopy Data is disposed of in a secure disposal bin or a crosscut shredder such that the information is no longer decipherable;
3. electronic Data is given to SonicWall's IT Asset Management team for proper disposal; and
4. appropriate technical measures are in place, including (without limitation): anti-virus software is installed on all systems; network protection is provided via firewall; network segmentation; user of content filter/proxies; interruption-free power supply; regular generation of back-ups; hard disk mirroring where required; fire safety system; water protection systems where appropriate; emergency plans; and air-conditioned server rooms.

DATA INPUT CONTROL. SonicWall has, where appropriate, measures designed to check whether and by whom Data have been input into Data processing systems, or whether such Data has been modified or removed.