



WEBROOT®



Customer Information Pack



Table of Contents

Introduction:	3
Commercial Terms*:	3
Personnel	3
Customer Data Migration At Termination:	4
Customer Data Migration During Contract:	4
Licensing Provisions:	4
Provisions for Information Security:	4
Data Protection Provisions*:	5
Provisions For Service Continuity*:	6
Hosting Strategy	6
Hardware Redundancy	6
Monitoring.....	6
Change Management	6
Provisions For Audit:	7
Service Dependencies*:	7
Complaints and Escalation Procedures:	7
Escalating Support Issues	7
Target Response Times.....	7
Escalation Contacts.....	8
Raising Complaints against Webroot.....	8
Cloud Industry Forum – Code of Practice Disclosures	9
Primary Contact Details:	9
Corporate Identity and Ownership Structure:.....	9
Scope of Business covered by the Code of Practice	9
Cloud Security Alliance	10
Code Compliance Policy Statement.....	10
Third Party Responsibility	10
Extended Commitments:	10
Certifications:.....	11
Conclusion	11



Introduction:

The following information is provided to add clarity and transparency to customers considering purchasing our Web, Email and Endpoint SaaS cloud services from Webroot Services Limited and to demonstrate our commitment to the Cloud Industry Forum's Code of Practice.

For confidentiality reasons additional information is available on request and under NDA, as required.

Commercial Terms*:

The following is a précised version of our Commercial Terms.

i. **Pricing Policy:**

UK pricing is in Pounds (GBP) and our Price List applies to new business. Renewals are processed based on rate and term of any existing contract, unless specified otherwise.

All our pricing is based upon per user per month, based on a minimum one year contract, and subject to minimum number of users and purchase price.

The minimum contract term is one year with additional years eligible for multi-year discounts which apply to all services (Web, Email, Archiving, Encryption, etc.) including all bundles and add-on module offerings.

ii. **Payment Terms:**

Our payment terms are normally set by our Reseller Partners, online payment is at time of purchase, or if for a larger number of users requiring a Purchase Order and Invoice within 30 days of invoice date.

iii. **Contract Lengths:**

Contract lengths are normally for 12 months, although contracts for 24 and 36 months with suitable discounts are also available. The initial Contract Term has an Effective Start Date and continues for the Subscription Term set out in our Contract Service Order.

iv. **Termination T&Cs:**

Under our Terms and Conditions either party may terminate the Agreement by providing the other party written notice at least thirty (30) days prior to the end of the applicable contract Term.

Termination may also be effected by not renewing the Agreement, if a party fails to cure any material breach.

v. **Renewal and Amendment Terms:**

At the end of the 'Initial Term' the Agreement is renewed automatically for consecutive renewal terms of twelve (12) months, unless terminated by either party by providing the other party written notice at least thirty (30) days prior to the end of the applicable Term.

Contracts can and may be amended with the agreement of all parties, for instance - to facilitate the co-termining of an additional service purchase to simplify renewals and future invoicing. This may only be agreed through a written document signed by both parties.

Personnel

Webroot employs c.450 employees worldwide at offices in the USA (HQ); Austria; Japan; Australia; Belgium; Ireland and the UK. Webroot Services Limited operates from two sites in the UK with software development centred in Derby and Support, Sales and Marketing in Bracknell, a total of c.50 staff.



In total there are 8 dedicated Enterprise Customer Support Personnel in the UK and 6 further Consumer Customer Support personnel are in Ireland.

Our Enterprise Support Staff have no access to Customer's administration management consoles without expressly granted individual access right permissions. Webroot conducts standard reference checks and vetting on its Support personnel.

Customer Data Migration At Termination:

Webroot does not normally hold customer data but processes their email messages and web searches through our SaaS servers to create real-time logs of the processing results according to each customer's policies. Webroot's view is that any data from a customer or generated as a result of processing a customer's data through our systems is their data.

Customers are always able to pull log files from us directly through their management portals, with web logs providing up to 12 months of log data and email up to 30 days of log data.

However in the case of Email Continuity and Email Archiving we do hold customer data in the form of their email messages, in the case of Business Continuity for a rolling 28 day period, and in the case of an email archive for as long as the customer requires.

There is no technological lock-in on a termination with a Customer able to access logs and export them as CSV files for importing into any other format and in the case of an email archive in the form they were originally provided i.e., a .pst file. In the case of archiving there is however an export fee that currently stands at c£6/GB.

There are no additional costs for exporting log data or need to export Business Continuity email messages.

Customer Data Migration During Contract:

Precisely the same Customer terms apply during the Contract as at a termination. Customers can freely download or request export of their logs on a regular basis.

Archived email is charged at £6/GB, but as all archived email is available through the administration portal and can be exported for Legal and eDiscovery free of charge the export charge rarely comes into effect for Customer's under contract.

Licensing Provisions:

Webroot Services Limited is entirely responsible for all of the software and licenses used in the provision of our SaaS security services and there are no other costs or licensing implications involved or obligations on either party.

Provisions for Information Security:

Webroot takes extremely seriously its responsibility for the secure operation of its SaaS datacenters and our entire security services infrastructure.

To ensure the security of our operations, and the customer data being processed there, we implement multiple layers of protection within our co-locations. This protection includes controls over personnel, access and change management controls, and the strict enforcement of security policies.



All team members are put through checks prior to receiving datacenter access privileges, and only select members of our datacenter team have physical or logical access to the SaaS production systems.

We secure our operations and data through stringent management policies. For example, if a change to the software or datacenter production environment is needed, it must first go through a change management process, which includes strict Quality Assurance (QA) and testing processes, before any production rollout. Webroot also tracks any system or applications changes through a dedicated change control application.

From a physical security perspective, our SaaS production servers and systems are situated in highly secure hosting centers in either a private cage setup, or with Amazon EC2 in their ISO and SAS70 accredited datacenters.

Webroot also mandates the use of state-of-the-art vulnerability assessment technologies to conduct regular vulnerability scans, and to ensure that any potential areas of risk are identified and promptly remedied.

We will continue to maintain strict internal data security standards, and have recently achieved independent SAS70 Type1 audit to validate our Webroot Web Security Services security standards.

As a SaaS 'cloud services' vendor we are totally committed to maintaining the security of our SaaS production systems, and will continue to make significant investments to ensure the continued confidentiality, integrity and availability of our entire global datacenter network.

Under NDA we are happy to make available a copy of our SAS70-1 audit for the Webroot Web Security Service and also our "Webroot® Datacenter Operations, Infrastructure and Security" that provides more details on datacenter infrastructure and the associated support, management and security processes used.

Data Protection Provisions*:

Webroot Services Limited provides by default the Webroot Email Security Service and the Webroot Email Archiving Service in the EU, within our UK and Eire datacenters. The Webroot Web Security Service uses a Global Load Balancing service to ensure the optimum user web performance for roaming and mobile users, which means processing users' web traffic logs is through the closest global datacenter.

Webroot recognizes that the content of all Emails sent or received, or Web Content uploaded or downloaded by Customers through our services, may be Confidential Information. In the normal provision of our services, Webroot will not access, read or copy Emails or attachments, or Web Content other than by electronic methods for the purposes of providing our services. Webroot has implemented industry standard procedures to:

ensure the security and confidentiality of Customer's Confidential Information;

protect against any anticipated threats or hazards to the security or integrity of such information; and

protect against unauthorized access to or use of such information.

The services provided by Webroot Services Limited are governed by the laws of England and Wales and subject to the UK Data Protection Act. Our Data Protection Act registration number is Z1895950.

We are also registered under the US Safe Harbor agreement, more details at:

<http://safeharbor.export.gov/companyinfo.aspx?id=9436>



Provisions For Service Continuity*:

Hosting Strategy

Within each geographical region serviced by Webroot, the core services are designed as fully redundant (N+1) solutions. The N+1 redundancy model is important because even if an entire datacenter is lost, all services will continue to operate without interruption— both in terms of web and email traffic flows and the preservation of access to static stored data (i.e., logs, reports, archives).

The SaaS infrastructure is hosted in state-of-the-art datacenters that are purpose-built to house mission critical data services applications. Each of our selected datacenters meets a strict set of guidelines in relation to building security, air conditioning, fire protection, physical access, connectivity to the internet backbone and power feeds.

Hardware Redundancy

Redundancy of infrastructure is a key requirement in achieving high availability. At a minimum, all selected equipment supports dual redundant power supplies. These power supplies are connected through PDUs (Power Distribution Units) to the datacenter's redundant power supplies, which operate on separated power circuits. Thereafter, individual machines utilize various RAID configurations for disk redundancy and NIC redundancy.

Monitoring

Even with state-of-the-art infrastructure, unplanned events still pose a risk to our services. With this in mind, Webroot operates a 24 x 7 monitoring platform through which every machine and infrastructure component is monitored. This monitoring platform covers disk capacity, availability, latency, checks for common failure scenarios, and other areas for concern. It also maintains historic data in relation to capacity, bandwidth, and queue sizes, which is invaluable for capacity planning and post-event analysis.

This all occurs within a Virtual environment, so even in the event of a major disaster, monitoring can deploy in a matter of minutes at a secondary location.

Change Management

To help maintain secure operations, all changes to the production system must be requested and approved through a rigorous and well-defined Change Management Process:

- a) **Backup Policies:** Detailed processes relating to backups of all core critical customer data, which are monitored on a weekly basis.
- b) **Incident Management:** In the event of unforeseen incidents, this process enables the incident to be managed in an effective manner and tracks through activities to ensure that the incident is mitigated in the future.
- c) **Access Management:** Strict multi-level access policies are maintained that detail the access rights of individuals to the core networks.
- d) **Risk Management:** Key risks to the operation of the service are managed on a month by month basis with a well-maintained risk register.



Provisions For Audit:

Webroot Services Limited is independently audited on a regular basis for compliance with its SAS70-1; FAST and PCI compliance. Plus, our datacenters are all audited and certified to the highest security standards.

Requests to arrange further independent security audits will be at the discretion of our CIO and other compliance audits the relevant Webroot Services Limited departmental head.

Service Dependencies*:

Webroot offers a minimum of 99.99% availability for all of our services taking into account the service dependencies we operate under. Webroot SaaS security solutions are dependent on Internet connectivity between the Customer and Webroot's datacenters, the correct Customer settings being in place, plus the availability of those datacenters and our email and web services processing infrastructure.

Our datacenters all offer multiple ISP Internet connectivity to ensure the Internet is always available, and our in-house Support will ensure that Customer settings are optimal for the use of our services. We structure our datacenter infrastructure on a Primary, Secondary and Tertiary set-up across different hosting providers, which provide excellent levels of availability, resilience and redundancy.

We therefore provide ongoing compliance with the Data Protection Act as email data always resides within the EU and very high guaranteed levels of business continuity, even in cases where the Customer's infrastructure is down†.

† If the Customer is subscribed to our email Business Continuity service.

Complaints and Escalation Procedures:

The escalation and the complaints procedure that is applied by Webroot Customer Services when providing assistance to our customers is as follows:

Escalating Support Issues

In the event that a workaround is not provided within the target workaround time, as indicated in the table of response times below, or you have a complaint of the service support you have received, then the following escalation timings and contacts apply. Escalation shall mean that the Customer may request access to a more senior member of the organisation in relation to the provision of the Workaround or complaint.

Target Response Times

When a support ticket is raised, we endeavour to work within the parameters defined below to complete a Customer call:

Category Level	Target Workaround From First Response
Critical	< 6 hrs Continuous work undertaken to workaround or fix. Work until it can be downgraded to a High Category
High	< 8 Hours of continuous work undertaken until it can be downgraded to a medium category
Medium	5 business days of continuous work undertaken until it can be downgraded to a low category
Low	7 Business days, provide a solution or a statement regarding the position of the problem



Escalation Contacts

If you feel that Webroot have failed to provide a satisfactory level of service based on the workaround targets, the Webroot Services Limited contacts for escalation are listed below:

Category Level	Support Supervisor Chris Saunders 0800 804 7015	Support Director Joanne Warner 0800 804 7015
Critical	4 Hours	8 Hours +
High	6 Hours	12 Hours +
Medium	5 Working Days	5 Working days +
Low	N/A	N/A

¹ Workaround means any of the following:

- a) resolution of the issue through the normal support process;
- b) a temporary by-pass of the issue;
- c) a statement that the issue will be considered for correction in a future upgrade;
- d) a statement that more information is required prior to resolution.

Raising Complaints against Webroot

In the event that there is the need to record a complaint, the following contacts applicable are:

Department	Name & Title	Email	Telephone
Service and Support	Chris Saunders Support Supervisor	csaunders@webroot.com	0800 404 7015
Service and Support	Joanne Warner Support Director	jwarner@webroot.com	0800 404 7015
Sales	Ian Moyse Channel Director	imoyse@webroot.com	0870 141 7070

Your enquiry will be treated with the utmost confidence and respect at all times.



Cloud Industry Forum – Code of Practice Disclosures

Webroot Services Limited is committed to the 'Code of Practice for Cloud Service Providers' (the 'Code') of the [Cloud Industry Forum](http://www.cloudindustryforum.org) (www.cloudindustryforum.org).

One of the main objectives of the Code is to help ensure disclosure of essential information so that consumers of Cloud Services can make better business decisions based on this information. The information on this page addresses the public disclosure requirements of the Code.

Primary Contact Details:

Company Name: Webroot Services Limited

Website: http://www.webroot.co.uk/En_GB/business.html

Contact: Mr. George Anderson

Title: Product Marketing, EMEA

+44(0) 203 349 2224 +44(0) 203 349 2224

Address: Venture House, Arlington Square, Bracknell, Berkshire RG12 1WA UK

Corporate Identity and Ownership Structure:

Webroot Services Limited is a privately held company and is a wholly owned subsidiary of Webroot Inc. based in Broomfield Colorado USA. Webroot is backed and owned by some of the security software industry's leading venture capital firms, including Technology Crossover Ventures, Accel Partners and Mayfield.

Board members include Dick Williams, President and CEO; Steve Cakebread; Quentin P. Gallivan; Theresia Gouw Ranzetta; Jake Reynolds and Robin Vasan. The Webroot Inc. Senior Executive Management Team consists of Dick Williams, CEO; John Post, CFO; Chris Benham, CMO; Gerry Cody CIO; Mike Malloy, Executive VP of Products and Strategy; Kenton Sieckman, VP of Worldwide Service and Support; David Huberman, General Counsel; Michelle Marian, Senior VP of Global Online Business.

Webroot Services Limited was formed in November 2002 as a limited company and is registered in England as company number 4597759.

Scope of Business covered by the Code of Practice

The Cloud Industry Forum Code of Practice applies to Webroot's SaaS (Software as a Service) cloud-based security solutions, and add-on services, offered through Webroot Services Limited and exclusively contracted with customers in the UK and Ireland.

The security solutions covered under the CIF code of practice are:-

1. **Webroot® Web Security Service** (shortly to be renamed **Webroot® SecureAnywhere™ Web Security**).
2. **Webroot® Email Security Service.**
3. **Webroot® Email Archiving Service.**
4. **Webroot® SecureAnywhere™ Endpoint Protection.**

Our SaaS cloud services are suitable for all public and private vertical sectors. For datacenter resilience and roaming and mobile user performance we operate a global infrastructure based in the UK, USA, Ireland, Australia, Sweden and Singapore. Local sales and support from Webroot Services Limited is available in the UK and Ireland.

Within our email services Customer's data is by default kept within the EU to clarify legal jurisdiction.



Cloud Security Alliance

Webroot are not members of the Cloud Security Alliance and have not participated or completed the Consensus Assessments Initiative Questionnaire. Details of our Security arrangements are however available on request, under NDA.

Code Compliance Policy Statement

Webroot Services Limited has completed the Self-Certification against the 'Code of Practice for Cloud Service Providers' (the 'Code') of the Cloud Industry Forum ('CIF', at www.cloudindustryforum.org). Clicking on the mark on our website will take you to the CIF website where supporting information for this Certification is available.

Webroot Services Limited is committed to the Code. One of the main objectives of the Code is to help ensure disclosure of essential information so that consumers of Cloud Services can make better business decisions based on this information. The information in this Customer Information Pack is intended to address the public disclosure requirements of the Code.

NOTICE: While Webroot Services Limited has made the commitment to the Code and has been self-certified as compliant with the Code, customers/third parties shall note that information or certification provided by the Cloud Industry Forum does not constitute advice from or endorsement by the Cloud Industry Forum. The Cloud Industry Forum disclaims any and all liability arising out of the use of services or otherwise of certified organizations. Where disclosed information or capabilities as specified by the Code of Practice are essential in purchasing cloud services from a certified organization, it/these should be cited contractually. Professional advice appropriate to specific circumstances should always be obtained.

Third Party Responsibility

Webroot accepts direct responsibility for all aspects of its SaaS cloud services provision, including those of our third parties, under the standard terms and conditions laid out within our Customer contracts.

We provide Customers' with guaranteed SLA's around the availability and resilience of our services that as a minimum guarantee 99.99% uptime. And, to avoid service or technical failures in our supply chain, Webroot operates our 'cloud' based services through different hosting providers. Architecturally, we operate Primary, Secondary and Tertiary processing in different locations to ensure no single points of failure and the continuous high availability of our SaaS services.

Webroot's suppliers do not have a direct or indirect responsibility to Webroot's Customers apart from under the terms laid out under our Master Services Agreement. In the circumstances of Webroot ceasing trading a refund would be made to customers' for the unused portion of their agreement and all data returned.

Should a Webroot Customer go into liquidation or administration, and a Customer of theirs request access to their data, we will (based upon proof of ownership and subject to any legal assignments or local regulatory restrictions) fully and timely comply with their request for their data.

In cases where a Customer's assets are legally transferred to another entity we will return the Customer's data to the new legal entity. Any discussions held with a Customer or their Customers' as a result of their administration or liquidation will be sympathetically and fairly based around the terms within our standard terms of contract.

Extended Commitments:

In addition to our commitment to the Cloud Industry Forum Code of Practice Webroot Services Limited is happy to provide relevant case histories and telephone customer references.

There are also full copies of our Master Services Agreement and SaaS Cloud solution SLAs may be found here: http://www.webroot.co.uk/En_GB/land-master-service-agreement.html



And, a Webroot Services Limited Cloud Industry Forum Customer Information Pack to clarify our key trading terms and conditions is available [here](#).

Certifications:

SAS70 -1 - Audit conducted by KPMG on the Webroot Web Security Service - April 2011. This audit is available on request under NDA. This supports the Provisions for Information Security required under the CIF Code.

PCI DSS Payment Card Industry Data Security Standard – Webroot is fully PCI compliant and all staff are tested and Webroot is audited annually for adherence to PCI compliance. This standard of information handling reflects Webroot’s due care of all customer data and the Provisions for Information Security required under the CIF Code.

ISO 27001/2 - Webroot partners with Amazon and their EC2 infrastructure to deliver our SaaS solutions. AWS’ Security Team has established an information security framework and policy based on the COBIT framework and is transitioning to a framework based on ISO 27002 controls. AWS Security maintains the security policy, provides security training to employees, and performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as conformance to the information security policy. They help to support the Data Protection and Provisions for Information Security required under the CIF Code.

Industry Memberships:

- FAST - Federation Against Software Theft, <http://www.fastiis.org/>
- EuroCloud, <http://www.eurocloud.org/>
- MSP Alliance, <http://mspalliance.com/>

Conclusion

This Customer Information Pack is applicable to Webroot Services Limited and is a demonstration of our transparency under the Cloud Industry Forum certification scheme. It will we hope assist you in considering the purchase of Webroot SaaS cloud security.

*Items marked with an asterix mean that further details on these items are available from our Master Services Agreement and the individual Webroot SLA and Service details which may be downloaded [here](#) or at:

http://www.webroot.co.uk/En_GB/land-master-service-agreement.html