Dr.Backup tm
online backup service

Network Security
Processes and Procedures Disclosure

For various reasons, we generally do not publicly release the detailed specifics related to our internal operations and security policies and procedures. However, we do understand some clients may need to have a deeper understanding of what precautions we take to safeguard their valuable data.

Please remember that our service to you is solely governed by our written service and software license agreements. These can be found online at: https://drbackup.net/service-agreement/. You can also find our web privacy policy at: https://drbackup.net/privacy-policy/.

The summary items presented below are for informational purposes only. Unless stated otherwise in our service agreement, the methods and techniques we discuss are subject to change without prior customer notice.

1. An overview of our basic security measures can be found here: https://drbackup.net/security/. Internally, we employ sophisticated **data encryption** methods and commercial grade **firewall and intrusion detection** services at the egress point of our network. This helps to protect our service and the security/availability of your data.

2. Our storage servers are collocated in a highly secure **SSAE-16 Type II certified carrier-grade data center**. Within this secure facility, all equipment is enclosed in a locked cage.

3. An annual certification of our data storage facility is prepared. We receive an **auditor's opinion letter** and **Service Organizational Control 1 Type II Report**. These documents detail testing performed and results observed. Distributions of these documents are highly-restricted and their examination is subject to execution of a strict confidentiality agreement.

4. We maintain and regularly review our internal **disaster recovery plan and procedures**. The goal is to enable us to resume operations at an alternate data center in the event of a physical disaster. However, any combination of natural disaster, technological failures and/or human activities may cause data loss – although we believe the chances of this to be extremely small.

5. We maintain **professional, general property, business continuity and "cyber" liability insurance** currently underwritten by a highly-reputable, U.S.-based insurance company. A declaration cover page can be provided upon an approved written request. Proper insurance coverage ensures we will have the financial stability to resume operations after a major disaster.

6. Due to the online nature of our business, we are subject to constant probing and attempted intrusion. To date, in our 15+ year history, to our knowledge there have been no successful penetrations of our secure production network. Should we become concerned about a possible network breach, we would provide general update notifications using the email we have for you

on file. Recommended actions (if any) would be provided.

7. Over the years, we have executed a large number of **HIPAA Business Associate Agreements** (BAA). These documents require us to observe a defined set of internal processes and procedures – and to formally notify impacted clients in the event of a data breach. Clients requiring specific personalized notification and disclosure may execute our standard BAA by completing this document: https://drbackup.net/whitepapers/DrBackup-HIPAA.pdf

   Note: We regret that our policy is to not execute any legally binding agreement that contains a financial indemnification clause.

8. All client data in transit and stored on our production servers is **FULLY ENCRYPTED**. In the event that our systems were electronically or physically compromised, our client data would remain highly-protected. Private encryption codes are maintained solely by the client (or their designated information technology consultant) and can be changed any time the client believes there is a risk of compromise.

9. We undergo **quarterly PCI penetration testing by an outside third party company**. The results of these tests are reviewed by our technical staff and receive action as appropriate. The results of these tests are highly confidential as they may disclose potential network vulnerabilities and recommend corrective procedures. See: https://drbackup.net/online-backup-general/the-importance-of-online-backup-security/ for an expanded discussion.

10. Both our server farm and disk storage arrays contain redundant components which help to ensure the highest levels of data availability. This includes the use of **RAID-6 disk technology** to provide you with access to your encrypted data -- even after the simultaneous failure of multiple volumes within a disk enclosure.

At Dr.Backup, we take great care to ensure the confidentiality, integrity and security of your valuable business data. The administrative, physical and technical safeguards detailed above represent some of the highest levels of protection you can obtain from a moderately priced commercial off-the-shelf product or service.