



## LIVEVAULT TECHNICAL BRIEF

### Security with LiveVault from Backup Direct™

Today more companies are recognizing the value and convenience of using online backup to protect their server data. If you are a network or information administrator, CIO or business owner considering the LiveVault Backup Service from Backup Direct™, then you may be wondering:

- How secure is my data? Could an unauthorized individual gain access to my data? Could my data stored with LiveVault be altered?
- Will my data be available when I need it? Is it safe from floods, fire or human error?

LiveVault addresses both of these concerns with the most secure solution on the market. All data is encrypted before it leaves your server and remains encrypted on the LiveVault vaults and optional TurboRestore appliances. Only you have access to the data encryption password. To insure the security and availability of data stored in vaults, LiveVault uses a fully redundant vaulting infrastructure at Iron Mountain's UK hosting facilities. These facilities provide stringent physical data protection safeguards.

#### Security for Data in Transit

LiveVault assures that the connection between your server and the Iron Mountain vaulting site is secure. LiveVault uses the best electronic security methods:

- *Automatic, outbound connections* - This means there is no added security risk to your environment. No changes are needed to your firewall configuration. The LiveVault Agent on your server only communicates with LiveVault vaults at the Iron Mountain data centre. The Agent initiates all communication and will find ports that allow outbound connections.
- *Public key encryption for mutual authentication* - There is no possibility of spoofing. The vault and the Agent independently validate certificates each time a connection is made. This authenticates the Agent to the vault and the vault to the Agent.
- *256-bit AES encryption of all data before transmission and storage* - This means there is no possibility of eavesdropping. Banks rely on this level of encryption. Data is also compressed for transmission and storage.
- *Digital signatures* – This means there is no possibility of corruption or modification. LiveVault digitally signs every packet. LiveVault detects any accidental or malicious modification, even if the underlying network protocols do not.
- *Web interface uses SSL* – The LiveVault web user interface is always protected through the Secure Sockets Layer (SSL).

#### Security for Data Stored in Vaults

Your encrypted data is vaulted at Iron Mountain UK data centres.

Your data is never stored at Backup Direct's offices. Security features of the data centres include:

- *Multi-level physical security* - two levels of security - building security and floor security. Visitors are escorted by security staff.
- *Hardened facilities* - Data centres meet numerous physical criteria including seismic specifications and intrusion resistance. Exterior walls are double reinforced concrete, and

are anonymous with no identifying signage. Concrete bollards are placed around the perimeter to prevent vehicles from penetrating an exterior wall. Conduits and walls are tightly sealed to prevent moisture intrusion.

- *Redundant and Backup Power* – There are dual utility power feeds from separate utility substations in underground duct banks, as well as redundant UPS power supplies and backup generators.
- *Redundant Network Connectivity* - Dual trunks from two different carriers enter the building from alternative distribution points. Plus redundant routers and switches.
- *Redundant HVAC* (heating, ventilation and air conditioning) – There is continuous monitoring with four-hour emergency response time service.
- *Advanced fire detection and suppression* – There is also under-floor leak detection.

**...highly resilient best-in-class Data Centres...that we could confidently showcase to customers...Iron Mountain.**

As a fully managed service, LiveVault complements the security offered by the data centre with its own infrastructure. LiveVault's Service Operations Centre (SOC) monitors and supports the LiveVault Service. Please note:

- *The SOC has no access to your data* – There is no possibility of decrypting your data. Only you have access to the data encryption password.
- *There is no access to data via the web user interface* – Furthermore, the LiveVault user interface only allows a restore to be done to the machine where the data originated, or to a server where you have installed the necessary data encryption key. (Data encryption keys must be installed locally.)
- *You can easily recover from a compromised data encryption key password with no data loss* - Any time you feel that a data password may be compromised, such as when a privileged employee leaves, you can change the password. This makes the old password inoperative with respect to any past or future data kept by LiveVault, but does allow you to access past and future backups with the *new* password. Changing a password does not cause any extra transmission of data from your server.
- *Redundant infrastructure* – LiveVault components such as firewalls, disks, vaults and web servers are implemented redundantly. There are always multiple copies of your data and LiveVault can quickly resume monitoring and support from another location if LiveVault's own SOC facility is lost or unavailable.

Today, over 1,500 customers rely on the security of the LiveVault Service to protect their data.

Data protected with the LiveVault Backup and Recovery Service is safer than it is in your own facility. LiveVault is the only company to guarantee recoverability of your data, while protecting the privacy and integrity of the data.

Visit [www.backupdirect.net](http://www.backupdirect.net) or call 08000 789 437 or email [sales@backupdirect.net](mailto:sales@backupdirect.net).