

NetBooks Security Policy
Last revised: August 29, 2007

The security of your data is very important to us. This Security Policy applies to the data uploaded by the businesses or other entities that subscribe to the NetBooks Application.

We protect customer data in a number of ways and have implemented an integrated hardware and software platform designed to maintain the ongoing confidentiality, integrity, and availability of all customer data uploaded to the NetBooks Application. Located in a dedicated colocation facility, our production systems are protected by 24x7 physical security, requiring positive visual ID, forfeit of driver's license, and multiple successful hand-scans to obtain access to the server cage. The NetBooks Application is run on a combination of best-in-class open-source and vendor-specific solutions.

Our security strategy includes the following:

- Secure Data Center
- SSL Encryption on all Client-Server Communications
- 24x7 Automated Server and Application Monitoring
- Internet Firewall
- Network Address Translation
- High-Availability Server and Network Infrastructures
- High-Availability Power Systems
- Secure Operating Systems
- Backup to Offsite Location
- High-Availability Application Design
- Redundant Customer Data Storage
- Separate Databases for Each Customer
- Latest Security Patches Applied as Needed

If you have any concerns about the security of your data, we invite your feedback at info@netbooks.com. Also note that we may update this security policy from time to time, and we will notify you of any material changes by posting the revised policy at www.netbooks.com/docs/public/sec. Please consult this policy regularly to stay informed of any changes.

Please note that this Security Policy is part of the NetBooks Service Agreement (available at <http://www.netbooks.com/legal>), which you should see for definitions of terms.