

GroveSite Security Overview

We at GroveSite understand concerns about data security and can assure you that GroveSite provides outstanding data protection. There are four key components to data security on our hosted service.

1. Physical Security

The GroveSite server farm is owned by GroveSite and does not host any unrelated businesses. We have complete control over our server equipment. The hardware is located in a top tier, 12,000 sq/ft datacenter owned and operated by OneNeck IT Services (www.oneneck.com). They provide fully managed operation of the servers including:

- 24x7x365 monitoring of all GroveSite servers and our connections to the Internet
- N+1 spare parts on premises for repairs
- Physical premise security including biometric hand scanners, card access and digital video security monitoring and logging
- Dry pipe fire suppression system with heat and smoke detectors in the sub flooring and ceiling
- Dual power distribution units, redundant power feeds, battery backup and on-site generator

2. Network and Operating Security

Included in the OneNeck IT Services managed services agreement is all platform level operational management of our servers. This includes:

- Daily full backup of all information, including regular off-site storage rotation
- Service pack and other vulnerability management
- Anti-Virus / Anti-Malware protection
- Firewall and network infrastructure protection from DoS and other Internet vulnerabilities

Note that GroveSite is not an archive service. GroveSite backups are primarily intended for our protection in the event of a massive hardware failure. If customers accidentally delete information off their sites, we may or may not be able to retrieve the information in a timely, cost effective manner. We do keep periodic snapshots of the environment, but we do not make any guarantee of recovering files deleted by users.

OneNeck IT Services undergoes an annual audit, performed by an independent service auditor, of the controls regarding Organizational and General Computer Controls, ERP Hosting, and Managed Services. The result of this audit is entitled SOC 1 Type 2 Report on Controls Placed in Operation and Tests of Operating Effectiveness. Please feel free to contact GroveSite for a copy of the latest audit report.

3. Application Security

GroveSite is responsible for ensuring the security of our web service application. This means we test for security vulnerabilities in our product which rides on top of the environment protected by OneNeck. This application level security is a top priority for GroveSite. Our business depends on customers knowing GroveSite is free from SPAM and other malware so common on websites today. We represent the safe option for web communities – no advertising, no “plug-ins”, no email marketing.

One of the ways we protect the security of our application is by reducing the exposed surface of our application thereby eliminating attack vectors. We do not provide lower level web publishing APIs such as WebDAV, FrontPage extensions, or even FTP – all of which have been full of security holes. Our model is simple and therefore can be more easily validated from a security standpoint.

For customers desiring secure communications over the Internet, GroveSite offers SSL encryption of all interaction with SSL-protected sites.

4. Account Security

Individual account security is usually the weakest link in any computing security scenario. We require ID and password login authentication for individual users to access their GroveSite team sites. You and your users need to follow good security practices. If people do not keep their passwords private and/or share accounts, the possibility for a security violation increases.

GroveSite offers a Strong Passwords option, whereby a customer may define minimum password length, required mix of character types, password expiration period, and so forth.

* * * * *

GroveSite Information Security Policy

Grove Technologies LLC (dba GroveSite) has a comprehensive written Information Security Policy that establishes the rules necessary to ensure the protection of confidential and/or sensitive information stored or transmitted electronically and to ensure protection of Grove Technologies information technology resources. The policy assigns responsibility and provides guidelines to protect the Grove Technologies systems and data against misuse and/or loss. Grove Technologies utilizes the ISO/IEC 27002:2005 (formerly known as ISO 17799:2005) as guidance for initiating, implementing, maintaining, and improving information security management as an IT internal control framework.

Please feel free to contact GroveSite to receive a copy of the Table of Contents for the GroveSite Information Security Policy.

If you should have any further questions about the security or reliability of GroveSite, please feel free to contact us directly.

GroveSite Support Team

866.952.9880 Option '2'

customerservice@grovesite.com