

SendThisFile® is a business unit of SendThisFile, Inc., a Wichita, Kansas U.S.A.-based corporation. SendThisFile® offers free accounts and paid accounts. This document only refers to paid accounts powered by the www.SendThisFile.com website, or operated on a SendThisFile® designated server.

FILE TRANSFERS

All SendThisFile® file transfers are protected with 128-bit encryption using Secure Socket Layer (SSL) technology. The SSL protocol was originally developed by Netscape, and eventually adopted by the Internet Engineering Task Force (IETF).

SSL provides SendThisFile® customers with two key security elements: (1) confirmation that the customer is communicating with the real SendThisFile® Web server at www.SendThisFile.com, and (2) the ability to encrypt file transfers.

SECURITY CONFIRMATION

When a SendThisFile® customer goes to <https://www.SendThisFile.com/>, the customer can click on the yellow lock that appears in the status bar of the customer's browser to confirm that the certificate for the SendThisFile® website is assigned to www.SendThisFile.com. This is the customer's proof that he or she is communicating with the real SendThisFile® website.

PAYMENT AND CREDIT CARD DATA

SendThisFile® is PCI DSS compliant (<https://www.pcisecuritystandards.org>). At no time does SendThisFile® store unencrypted credit card numbers on our servers. The credit card verification code (CVV2, CVC2, CID, or CAV2) is never stored and only used for the initial payment. All payment processing communication uses SSL utilizing only High Strength Encryption Ciphers.

DATA SECURITY

SSL allows a customer's browser, and our Web server, to exchange public keys so that data transferred between the two computers can be properly encrypted and decrypted. No one on any of the networks transporting packets between SendThisFile® and our customer's browser will be able to reconstruct the original files that have been sent.

STORED FILES

Enterprise and Business Plan holders have the option of allowing or requiring end users to store the files on our servers as encrypted files. The purpose of this encryption is to make sure that a file is secure, even in the event that one of our servers is compromised. The sender should keep a copy of the file until they have confirmation that the recipient has successfully received it, opened it, and used it—because if there is an error in the process our support staff may not be able to help recover the file.

Files that are encrypted on-the-fly by our system do not require the sender to encrypt the files on their computers first. Files are decrypted on-the-fly so the recipient receives an exact, decrypted, copy.

The type of encryption used for the storage of files is the Advanced Encryption Standard (AES) as described in FIPS PUB 197. We are currently using a 128-bit encryption key for the file streams.

Only four principals of SendThisFile, Inc. have access to the code that would be necessary to decrypt a file.

TRANSFER IDs

Files are tracked by a unique, randomly generated key called a transfer ID. Transfer IDs are 24 characters (192 bits) in length and can be any combination of uppercase English alphabet characters, lower case English alphabet characters, or the 10 numeric characters. (This set of characters is known as the alphanumeric character set.) There are 62 characters in the alphanumeric character set.

When a file is uploaded, an email is sent to the recipient's password-protected email account with two key pieces of information: A URL encoded file name and a transfer ID. The SendThisFile® download page requires that the transfer ID be valid before a download is allowed.

If a malicious user tries a brute force attack to guess a SendThisFile® transfer ID, it would take on average $\frac{62^{24}}{2} = 1.115 \times 10^{43}$ guesses. If a person had a network fast enough to try a billion guesses per second, it would take 3.5×10^{26} years to guess a transfer ID. Enterprise Plan files are removed from the SendThisFile® system after 14 (fourteen) days, so there is ample security here.

FILE SYSTEM / SERVER ACCESS

Our servers all run secured versions of RedHat Linux. To minimize attacks, all network services have been turned off on all servers except for the following:

PORT	SERVICE
80	Caucho Resin
443	Caucho Resin
110	POP-3
1521	Oracle Listener
22	SSH
25	SMTP

Our developers only have access to our development systems, which requires two factor authentication. Only the principals of SendThisFile, Inc. and authorized server administrators have access to our production systems.

Audit logs of our operating system logins are sent to the principals of SendThisFile, Inc. on a nightly basis in order to make sure that our servers haven't been compromised.

All file servers are running file integrity scanning software. The results of those scans are sent to the principals of SendThisFile, Inc. for analysis on a daily basis.

Monthly vulnerability scans are performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Internal vulnerability scans are performed at least quarterly but are also executed for any major system or network change.

LOGS

All uploads and downloads are recorded in our database, whether or not they were successful. This includes the file up/downloaded, the date and time, and the IP address of the sender or recipient. Enterprise Plan customers can set up multiple administrators that have the ability to remove files from the SendThisFile® system in the event that a file is uploaded to the SendThisFile® server in error, however, these administrators cannot access the file.

The corporate originator of the account has complete control over the files. That means that the owner of the account (the corporate originator) can remove, and access, all the files within the account.

DOMAIN CONTROL

Our Enterprise Plan customers may add as many domains as they wish to a list of "Valid Domains". The domains are compared to the senders and recipients of files on the customized "send this file" page. In order for a transaction to take place, either the sender or the recipient of the file must be associated with one of the valid domains.

ACCOUNT HOLDER CONTROL

Enterprise Plan holders can require that the sender be a registered and verified SendThisFile® account holder. When sending a file on the Enterprise Plan's branded upload (send) page, the sender will be required to enter the password for their registered and verified SendThisFile® account. This prevents someone from sending a file as somebody else in the same company, because the sender can only send files from the SendThisFile® account to which they have access. Even though the registration process for this upload (send) page ultimately creates a SendThisFile® account, the registration process is completely branded using the Enterprise Settings page, so it appears to the sender as if the sender holds an account with the Enterprise Plan holder.

FILE DELETION POLICY

The standard file deletion time for paid customers is based on the selected plan (up to a default of fourteen days for Enterprise Plans). Enterprise Plan holders can reduce or extend this period via the Enterprise Settings page.

WE DO NOT BACKUP ANY FILES THAT ARE TRANSMITTED OVER OUR SYSTEMS, so there is no possibility of sensitive files being stored on archival media (such as tape), and thus being compromised by third party storage companies.

We are continuously sending archive logs from our primary database to a remote backup database. The database does not store any customer files in partial or in whole. The database only contains account information, and file transfer logging information.

NONDISCLOSURE AGREEMENTS

We have a Nondisclosure Agreement *for Computer File Transmissions* that we will sign for our Enterprise Plan customers at their request.

Aaron Freeman
Michael G. Freeman
John W. Stephens
Scott E. Sexton

Copyright 2003-2011 by SendThisFile, Inc. All rights reserved.

REVISION HISTORY

- *Original: Aaron Freeman, Michael Freeman, John Stephens*
- *Revision 8 - 01 May 2010: Aaron Freeman, Scott Sexton*
- *Revision 9 - 01 Jul 2010: Aaron Freeman, Scott Sexton*
- *Revision 10 – 04 Oct 2010: Aaron Freeman, Scott Sexton*
- *Revision 11 – 17 Jan 2011: Scott Sexton*
- *Revision 12 – 7 Jul 2011: Aaron Freeman*