



Summary of Activator Architecture, Security & Data Safeguards

This document provides an overview of the architecture, privacy and security measures used in the Activator System to fully safeguard data and to ensure that what is yours stays in your control at all times. Turnkey is constantly making extensive efforts to exceed the security standards recognized by the computing industry today.

Table of Contents

Physical Security and Data Integrity 2

- Network Security..... 2
- Data Integrity 2

Internet Security 3

- SSL..... 3
- Encryption 6
- Intrusion Monitoring..... 6
- Intrusion Testing..... 7

 - Integration with Activator Website 7
 - Trustwave – TrustKeeper External Vulnerability Scan..... 8
 - About Trustwave 9
 - TrustE Certification..... 9

Application Security..... 10

- Channels 10
- User Access 10

Security Bolstered by Terms of Use 12

- Identity Safeguards 12
- Data Safeguards..... 12
- Confidentiality..... 13
- Intellectual Property 13

Physical Security and Data Integrity

Network Security

Turnkey's Activator site is situated in a secure facility staffed with 24-hour, electronic key-card accessed employees. The network on which the site is hosted is protected by an industry standard firewall, with all access strictly controlled. All non-http access into the network location is strictly controlled by advanced security measures, including VPN-controlled access, secure FTP access (no standard FTP access), and/or IP address restrictions.

Data Integrity

The application environment is supported by clustered servers, automatic failovers, load balancers, and log shipping as per industry standard procedures. Activator is hosted in two SSAE 16 compliant datacenters that are located in separate geographical regions of the country. Turnkey's Disaster Recovery Plan provides protections and policies to keep your data online in the event of a catastrophic disruption at one of our data centers.

The data stored on Turnkey's servers are backed up in a standard backup rotation, with data eventually going to tape and being stored in a secure temperature-controlled facility for a short period to enable disaster recovery. This process is standard procedure, and is performed by highly respected companies following an industry standard disaster recovery methodology.

Internet Security

SSL

Turnkey has secured an Enhanced Validation (EV) Secure Socket Layer (SSL) certificate for the TurnkeyActivator.com website. SSL is the standard mechanism by which any website gains the ability to communicate via a secure connection (which shows in a browser as “https://” vs. “http://”) that provides encryption of the *content* of a communication between a web server and a browser.

Turnkey has taken steps exceeding industry standards wherever possible to ensure data security, and the SSL certificate is no exception. The SSL certificate used for Turnkey’s Activator website uses industry-leading 2048-bit encryption (for browsers that accept it), far exceeding the minimum 40-bit encryption and even the industry standard 128 or 256-bit encryption. Going a step further, Turnkey has secured an Extended Validation SSL certificate. As explained by the Comodo website, “The green browser address bar, exclusive to EV SSL certificates, assures website visitors that they are transacting on a highly trusted and secured domain. The EV SSL certificate was designed to strengthen e-commerce security and combat phishing attacks to make EV SSL the most complete SSL certificate available.”

The PCI DSS (Payment Card Industry Data Security Standard) is an information security standard for organizations that handle cardholder information (http://en.wikipedia.org/wiki/PCI_DSS). Turnkey does not deal with credit cards on the Activator website, yet the site still meets all requirements for PCI certification. Basically, even though Turnkey does not perform any transactions on the Turnkey Activator website that require PCI certification (which is specifically targeted at credit card transactions on e-commerce sites), we decided that our website would be at *least* as secure as if we did. The EV SSL certificate far exceeds the requirements to gain a PCI certification.

An EV SSL certificate displays the company’s name in the browser bar to provide additional validation of the site’s authenticity. When visiting our site, users can verify that Turnkey Sports LLC is hosting and providing the Activator application. EV SSL is becoming the new standard for verifying a site’s authenticity.



More detail on the importance and usage of EV SSL (from http://en.wikipedia.org/wiki/Extended_Validation_Certificate):

ACTIVATOR

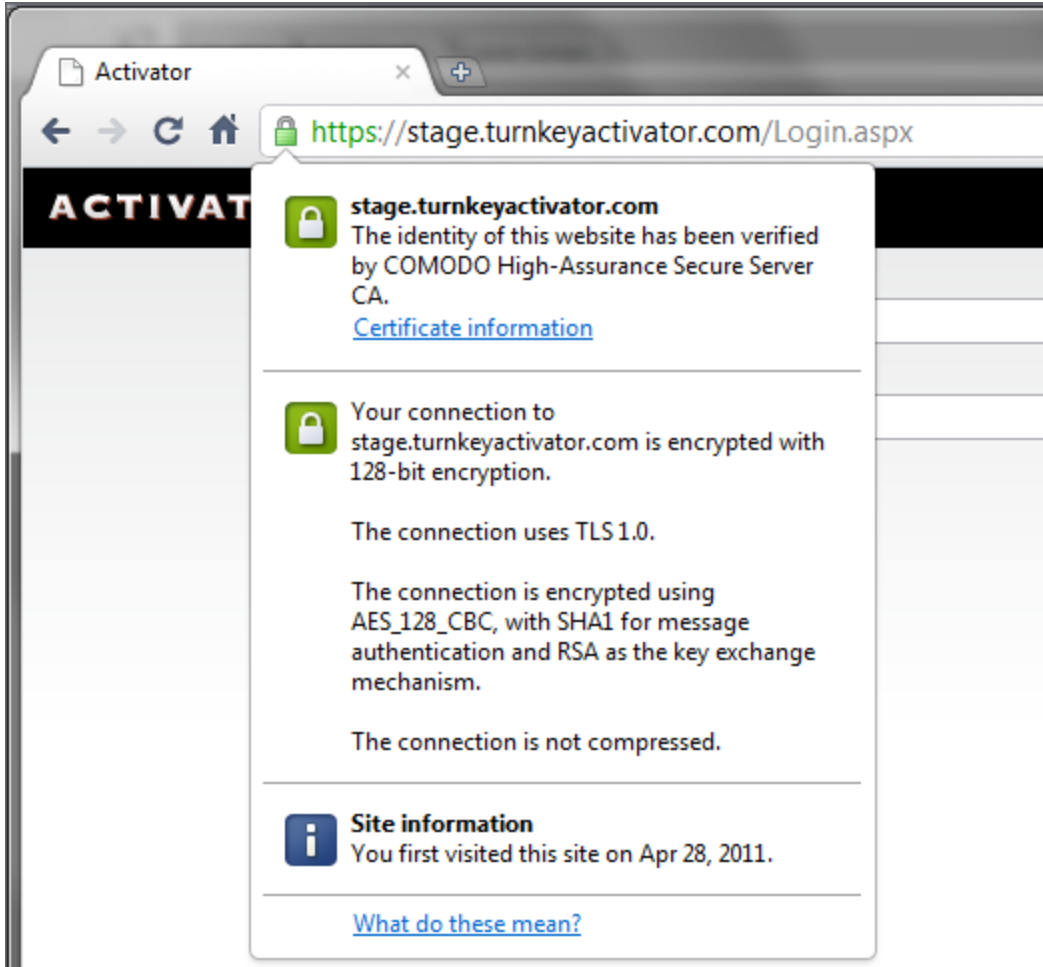
An important motivation for using digital certificates with SSL was to add trust to online transactions by requiring website operators to undergo vetting with a certificate authority (CA) in order to get an SSL certificate. However, commercial pressures have led some CAs to introduce "domain validation only" SSL certificates for which minimal verification is performed of the details in the certificate.

Most browsers' user interfaces did not clearly differentiate between low-validation certificates and those that have undergone more rigorous vetting. Since any successful SSL connection causes the padlock icon to appear, users are not likely to be aware of whether the website owner has been validated or not. As a result, fraudsters (including phishing websites) have started to use SSL to add perceived credibility to their websites.

By establishing stricter issuing criteria and requiring consistent application of those criteria by all participating CAs, EV SSL certificates are intended to restore confidence among users that a website operator is a legally established business or organization with a verifiable identity.

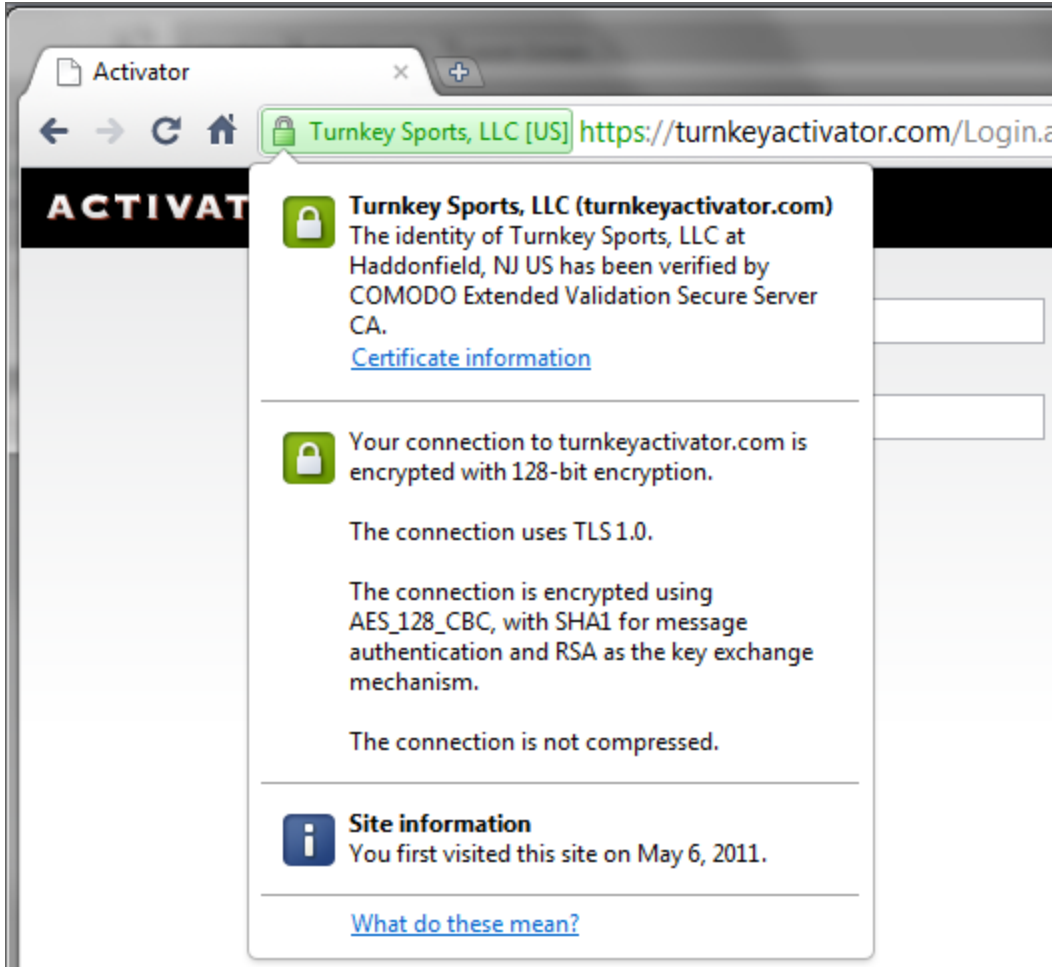
Further validation can be provided by clicking on the lock icon. A normal SSL simply confirms that the site's identity has been validated:

ACTIVATOR



The EV SSL confirms the identity of Turnkey Sports in Haddonfield NJ as the owner of this site. The difference is a small distinction, but provides the extra layer of authenticity that is lacking from normal SSL.

ACTIVATOR



Encryption

All interactions with the Turnkey Activator website have been designed with security as a primary concern. All interactions directly with database objects are done with specific regard to avoiding revealing any information in publicly visible means (such as URL sniffers or other hacking tools.) If there is a case on the website where information must be passed in a URL, that URL is “aged”, allowing temporary access only, as well as encrypted by RSA encryption to foil any attempts to gain unauthorized access to the system.

Intrusion Monitoring

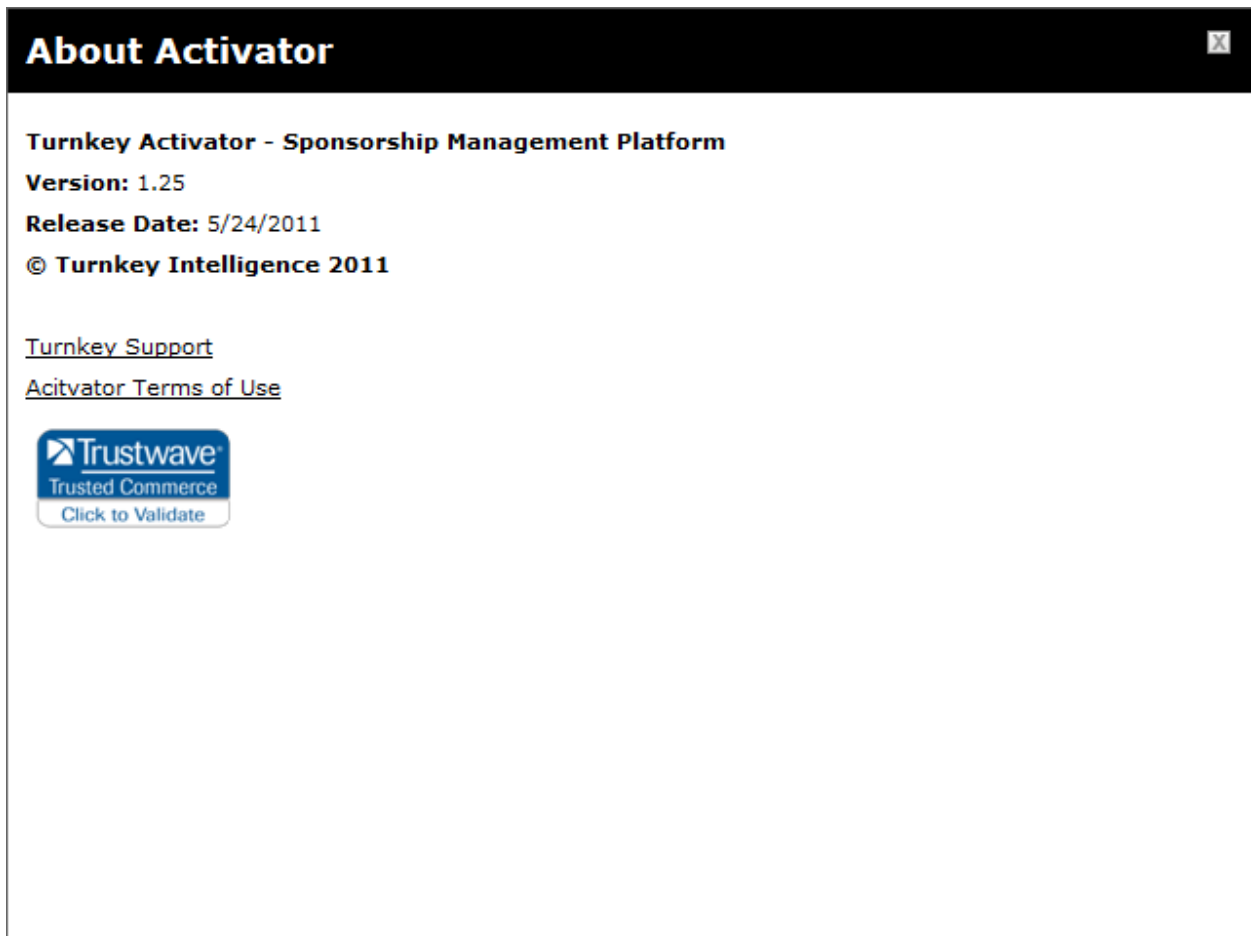
The Turnkey Activator website is monitored 24 hours a day, seven days a week, both automatically by standard monitoring software, but also by staff in our secure hosting facility. The staff is trained to spot any intrusions, denial of service attacks, or even general site problems, and have 24 hour access to top Turnkey staff members in case of problems.

Intrusion Testing

TrustKeeper scanning is being used to verify our compliance with PCI DSS guidelines on network security. Network compliance is one piece of the larger PCI DSS standard.

Integration with Activator Website

The TrustKeeper seal appears on the “About” page of Activator:

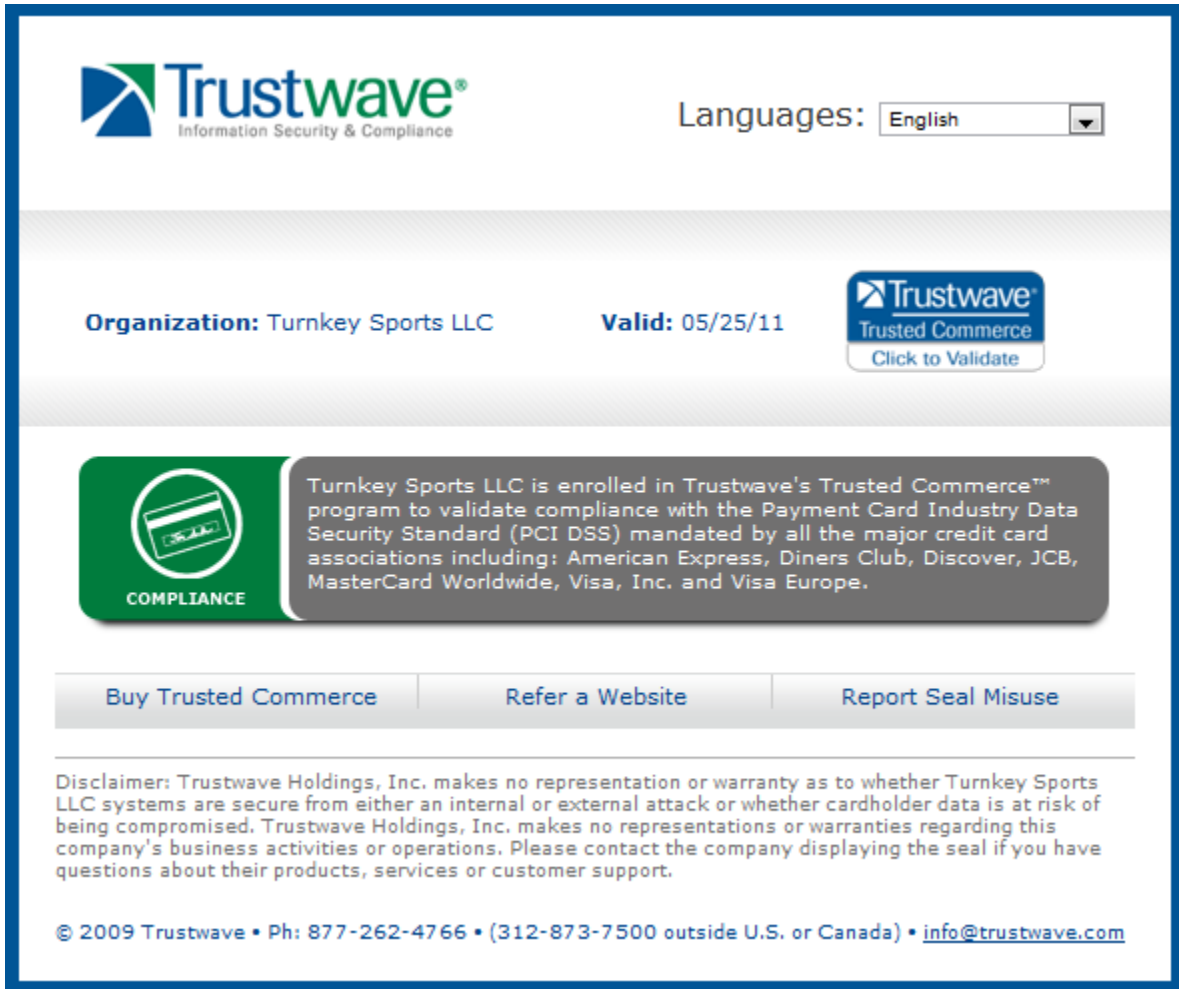


Clicking on the Trustwave logo will take the user to Trustwave’s website where our compliance can be verified. The verification is available at:

<https://sealserver.trustwave.com/compliance/cert.php?code=w6olF7WieJraVGclPlh8RytnQ669qi&style=invert&size=105x54&language=en>

ACTIVATOR

Visitors to this site will see our Organization name, last scan date, and whether our site is compliant with the guidelines.



The screenshot shows a Trustwave Trusted Commerce seal. At the top left is the Trustwave logo with the tagline "Information Security & Compliance". To the right is a "Languages:" dropdown menu set to "English". Below this, the organization name "Turnkey Sports LLC" and the validity date "Valid: 05/25/11" are displayed. A "Click to Validate" button is also present. A central banner features a green "COMPLIANCE" icon and text stating: "Turnkey Sports LLC is enrolled in Trustwave's Trusted Commerce™ program to validate compliance with the Payment Card Industry Data Security Standard (PCI DSS) mandated by all the major credit card associations including: American Express, Diners Club, Discover, JCB, MasterCard Worldwide, Visa, Inc. and Visa Europe." Below the banner are three buttons: "Buy Trusted Commerce", "Refer a Website", and "Report Seal Misuse". A disclaimer at the bottom reads: "Disclaimer: Trustwave Holdings, Inc. makes no representation or warranty as to whether Turnkey Sports LLC systems are secure from either an internal or external attack or whether cardholder data is at risk of being compromised. Trustwave Holdings, Inc. makes no representations or warranties regarding this company's business activities or operations. Please contact the company displaying the seal if you have questions about their products, services or customer support." At the very bottom, contact information is provided: "© 2009 Trustwave • Ph: 877-262-4766 • (312-873-7500 outside U.S. or Canada) • info@trustwave.com".

Trustwave – TrustKeeper External Vulnerability Scan

(from <https://www.trustwave.com/vulnerabilityScanning.php>)

Vulnerability scanning can help secure your network and your information by proactively identifying weaknesses in your security posture. Trustwave specializes in helping organizations discover and understand their security vulnerabilities before hackers can exploit them.

Trustwave scans are designed to detect more than 5,000 known network, operating system and application vulnerabilities - including the SANS Top 20 -- and are executed without any impact on your devices. That is why more merchants, payment processors and

ACTIVATOR

acquiring banks have worked with Trustwave to manage their Payment Card Industry Data Security Standard (PCI DSS) compliance validation programs.

Our on-demand compliance management portal, TrustKeeper®, is designed to detect and alert you of security flaws at your network perimeter and provide guidance to address these exploits. External vulnerability scanning with TrustKeeper is a requirement to meet the security requirements of several industry and regulatory standards including the PCI DSS.

About Trustwave

(from <https://www.trustwave.com/aboutus.php>)

Trustwave is the leading provider of on-demand data security and payment card industry compliance management solutions to businesses and organizations throughout the world. Trustwave has helped thousands of organizations — ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers—manage compliance and secure their network infrastructure, data communications and critical information assets.

TrustE Certification

In addition to the certifications mentioned above, Turnkey also holds a TrustE certification for TurnkeyActivator.com. In the absence of the capture of cardholder information, Turnkey sought out TrustE as a certification program similar to the PCI DSS to provide our customers with the confidence that a PCI DSS would provide if we were to capture cardholder information.

The TrustE certification program involved verification of many of the features mentioned above, in addition to full verification of Turnkey as a company and all of our physical security.

Please visit TrustE's website at <http://www.truste.com/privacy-program-requirements/index.html> for more information about the TrustE certification.

Application Testing

Application security is tested using the Cenzic Hailstorm penetration testing application. Application scans are completed at the end of every development cycle. Scans are also completed on a weekly basis to ensure the production environment is secure.

Application Security

Application security is a level of security applied to secure data at the level of the actual web page. Turnkey took on the difficult challenge of creating a website designed to be completely secure and, simultaneously, facilitate collaboration and content sharing content between multiple parties. Everything in the Turnkey Activator system was built with security in mind. Below is a quick summary of some of the concepts of the Activator application that make sharing possible with the highest regard for security. For a more complete explanation of the application security in terms of overall concepts, please visit <http://support.turnkeyactivator.com/forums/214203-glossary-of-terms>.

Channels

(From <http://support.turnkeyactivator.com/entries/434553-channel>)

Within Activator, the term Channel refers to a marketing partnership or relationship between two entities. An Activator Patron creates one (1) unique Channel for each marketing partnership he or she wishes to manage within Activator.

An Activator patron may wish to create a Channel to be used as an internal partnership management resource. In this scenario, the Channel created is a "One-Way Channel". In the case of a One-Way Channel, the Patron's Channel Partner (i.e., the entity whose relationship with the Patron is being managed via the Channel) cannot access the Channel. The Channel Partner may not even be aware of the Channel's existence.

The second type of Channel is called a "Shared Channel" or "Two-Way Channel". After creating a Shared Channel, the Activator Patron will invite his/her Channel Partner onto the Channel as a "Recipient". That Channel Partner then has access to all "shared" content on the Channel, and is given the ability add Channel content, users, etc.

Upon signing in to Activator, the first screen you see is Activator's Channel Wall. At this point, all of your existing Activator channels have been pre-selected. To modify your channel selection and only view content associated with/work within a specific channel or group of channels, click the downward-pointing arrow located on the portfolio button labeled "All Channels". This is your "channel picker"; use it whenever you'd like to select or de-select one or more Activator channels.

User Access

(from <http://support.turnkeyactivator.com/entries/239421-permissions-view-create-share>)

ACTIVATOR

When setting up Activator users, you have the opportunity to control each user's access to different types of content, and limit his/her ability to make modifications to that content by applying one or more of the following permission levels:

- View
- View/Create
- View/Create/Share

View is Activator's most basic permission level. Applying only the view control ensures that a user can only read (or "view") Activator items. When given only the view permission level, a user will not be able to create, edit, share, or delete items within Activator.

If a user is given the view/create permission, that user will have the ability to view, create, and edit/modify items within Activator. However, the user remains unable to share items with his/her channel partners.

The view/create/share permission is Activator's most powerful permission. If a user is given the view/create/share permission, he/she can view content, create and edit items within Activator, and share items with channel partners.

To set or modify a user's permission level, sign into Activator and click the "Settings" link found in the upper right corner of the Activator site. Then, select "Users" from the left-side menu and click the user whose permissions you wish to modify. You can then modify their permissions from the "Details" tab.

Channel access (i.e. which channels a user may access) is controlled by Administrative users.

Security Bolstered by Terms of Use

Activator requires all users to agree to the exact same Terms of Use, meaning that all users on the platform are working under the same rules of the road. As such, those Terms of Use serve and support several important purposes, including:

1. Codifying Turnkey's security commitments into enforceable contractual commitments
2. Codifying Activator's privacy controls into enforceable confidentiality commitments
3. Codifying Activator's use restrictions into strict contractual prohibitions applicable to not only Turnkey but also to all other users in the Activator "community"

Identity Safeguards

Every user agrees in advance to register with Activator by providing true, accurate, current and complete information and maintaining and promptly updating said information to keep it true, accurate, current and complete. Every user is responsible for all activities that occur under his or her account, whether or not such activities were expressly authorized by the user. Every user agrees not to use, or permit any other person to use his or her name, password, login or any other information. Every user agrees not to disclose, directly or indirectly, in whole or in part, any other Person's account information to any third party.

Data Safeguards

TI contractually commits to "aggressively safeguard all Activator Data by maintaining industry standard safety and security measures including, at a minimum: (i) hosting all Activator Data in a primary hosting facility that meets or exceeds all standards required for a SSAE 16 Type II certified facility or comparable; (ii) performing network security testing no less than monthly; (iii) performing application security testing no less than weekly; (iv) maintaining a full disaster recovery environment in a separate geographic location/facility that meets or exceeds the standards required for a SSAE 16 Type II certified facility or comparable; (v) supporting synchronization of Activator Data between the primary hosting facility and the disaster recovery environment no less than daily; and (vi) backing up all Activator Data to disk no less than daily and to tape no less than weekly."

Every user agrees to not share data with any person, unless expressly authorized in advance by the owner of such data to share that data with such person.

ACTIVATOR

Every user agrees to not introduce into Activator any virus, Trojan horse, worm, or other mechanism intended to cause the destruction, loss, interception or alteration of data by unauthorized means and/or persons.

Confidentiality

Turnkey and every user agree not to disclose Confidential Information to any other person and agree to protect and treat all Confidential Information with the highest degree of care. Turnkey and every user expressly agree to not use or make any copies of Confidential Information of any person, directly or indirectly, in whole or in part, without the prior written authorization of such person. These contractual obligations continue for five (5) years following termination or expiration of any user's license.

Intellectual Property

Activator does not address, amend, modify, transfer and/or otherwise impact in any way any pre-existing right, title and/or interest in and to your User Data or the Activator Data. Any Person with a pre-existing right, title and/or interest in any data prior to it being brought into Activator retains all said pre-existing right, title and interest in and to said Data.