Cookie Policy

TCS Empowers uses cookies (small text files placed on your device) and similar technologies to provide our websites and to help collect data. The text in a cookie often consists of a string of numbers and letters that uniquely identifies your computer, but it can contain other information as well.

Our Use of Cookies and Similar Technologies

TCS Empowers uses cookies and similar technologies for several purposes, which may include:

- Storing your Preferences and Settings: Settings that enable our website to operate correctly or that maintain your preferences over time may be stored on your device.
- Sign-in and Authentication: When you sign into our website using your credentials, we store a unique ID number, and the time you signed in, in an encrypted cookie on your device. This cookie allows you to move from page to page within the site without having to sign in again on each page. You can also save your sign-in information, so you do not have to sign in each time you return to the site.
- Security: We use cookies to detect fraud and abuse of our websites and services.

Does TCS Empowers use cookies for analytics?

When we send you a targeted email, subject to your preferences, which includes web beacons, cookies or similar technologies we will know whether you open, read, or delete the message.

When you allow the Performance Cookies to be dropped on your browser, we can associate cookie information with an identifiable individual. For example:

- When you click a link in a marketing e-mail you receive from us or fill up a form on our website, we will also use a cookie to log what pages you view and what content you download from our websites.
- Combining and analysing personal data – We may combine data collected from performance cookies dropped on your browser. We use this information to improve and personalize your experience with our websites, provide you with content that you may be interested in, create marketing insights, and to improve our business and services.

In addition to the cookies TCS Empowers sets when you visit our websites, third parties may also set cookies when you visit TCS Empowers' sites. In some cases, that is because we have hired the third party to provide services on our behalf.

reCAPTCHA

We use reCAPTCHA service, a security service that stops bots and other automated attacks, on all TCS Empowers sites to protect our platform. The service watches over all users' actions across all our sites to determine if they have any malicious intent. No additional personal information is taken from our users to enable this service.
reCAPTCHA is used to:

- Fight spam and abuse against our users' property and the TCS Empowers platform.

- Detect any abusive traffic on TCS Empowers.

reCAPTCHA is not used for:

- Sharing user information to any third parties.
- Providing third parties with information to support advertising, determining credit worthiness, employment eligibility, financial status, or insurability of our users.

COOKIE DETAILS

Some of the cookies we commonly use are listed below. This list is not exhaustive, but it is intended to illustrate the main reasons we typically set cookies. If you visit one of our websites, the site may set some or all of the following cookies.

Cookie Name	Description	Party	Cookie Category	Domain	Expiry
XSRF-TOKEN	XSRF-TOKEN cookie is used to prevent CSRF attacks. CrossSite Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application. This cookie allows the browser to manage the browsing session and keep it alive for as long as it is needed	First party	Strictly Necessary Cookies	tcsempowers.tcsapps.com	Session
connect.sid	connect.sid is a unique, randomly generated number that stores the session cookies. Session cookies track the user's behavior on the website and help websites identify users browsing through the web pages of a website. General purpose platform session cookie, used by sites written in Node & Express. Usually used to maintain an anonymous user session by the server.	First party	Strictly Necessary Cookies	tcsempowers.tcsapps.com	Session

_csrf	_csrf token is a secure random token (e.g., synchronizer token or challenge token) that is used to prevent CSRF attacks. The token needs to be unique per user session and should be of large random value to make it difficult to guess. A CSRF secure application assigns a unique CSRF token for every user session.	First party	Strictly Necessary Cookies	tcsempowers.tcsapps.com	Session
Optanon Consent	This cookie is set by the cookie compliance solution from OneTrust. It stores information about the categories of cookies the site uses and whether visitors have given or withdrawn consent for the use of each category. This enables site owners to prevent cookies in each category from being set in the user's browser when consent is not given. The cookie has a normal lifespan of one year, so that returning visitors to the site will have their preferences remembered. It contains no information that can identify the site visitor.	First party	Strictly Necessary Cookies	tcsempowers.tcsapps.com	Session

Optanon AlertBox Closed	This cookie is set by websites using certain versions of the cookie law compliance solution from OneTrust. It is set after visitors have seen a cookie Banner and, in some cases, only when they actively close the notice down. It enables the website not to	First party	Strictly Necessary Cookies	tcsempowers.tcsapps.com	Persistent

	show the Banner message more than once to a user. The cookie has a oneyear lifespan and contains no personal information				
ApplicationGatewayAffinity	This cookie allows the browser to manage the browsing session and keep it alive for as long as it is needed.	First party	Strictly Necessary Cookies	tcsempowers.tcsapps.com	Session
__cfduid	This domain is owned by OneTrust, a privacy management software which helps organizations achieve compliance with global regulations.	Third Party	Strictly Necessary Cookies	onetrust.com	Persistent
at_check	A simple test value used to determine if a visitor supports cookies	First party	Performance Cookies	tcsempowers.tcsapps.com	Session
sc_dslv	Determines the number of days since a user last visited your site and captures this information in an Analytics variable.	First party	Performance Cookies	tcsempowers.tcsapps.com	Persistent
mbox	This cookie is used to give website operators the ability to test which content is more relevant to visitors.	First party	Performance Cookies	tcsempowers.tcsapps.com	Persistent
s_sq	This cookie contains information about the previous link that was clicked on by the user.	First party	Performance Cookies	tcsempowers.tcsapps.com	Session
s_ppvl	Store information about percentage of page displayed	First party	Performance Cookies	tcsempowers.tcsapps.com	Session
s_ppv	Store information about percentage of page displayed.	First party	Performance Cookies	tcsempowers.tcsapps.com	Session
sc_dslv_s	Determines the number of days since a user last visited your site and captures this information in an Analytics variable,	First party	Performance Cookies	tcsempowers.tcsapps.com	Persistent

gpv_pn	Captures the value of an Analytics variable on the next page view.	First party	Performance Cookies	tcsempowers.tcsapps.com	Persistent
s_plt	Tracks the time that the previous page took to load	First party	Performance Cookies	tcsempowers.tcsapps.com	Session
s_tp	Tracks percent of page viewed	First party	Performance Cookies	tcsempowers.tcsapps.com	Session
s_ips	Tracks percent of page viewed	First party	Performance Cookies	tcsempowers.tcsapps.com	Session
category_id	The purpose of this cookie is to identify the preference of the user. Based on the previous 3-page navigation done by the user, AI will predict in which cluster the user belongs to. And this cluster information is stored as a cookie. Cards as per the users' interest are shown based on this cookie value.	First party	Functional Cookies	tcsempowers.tcsapps.com	Persistent
UUID	This cookie is used to identify a repeat user on the website	First party	Functional Cookies	tcsempowers.tcsapps.com	Persistent
li_fat_id	Member indirect identifier for Members for conversion tracking, retargeting, analytics	First party	Targeting Cookies	tcsempowers.tcsapps.com	Persistent
VISITOR_INFO1_LIVE	This cookie is used as a unique identifier to track viewing of videos.	Third Party	Targeting Cookies	youtube.com	Persistent
YSC	YouTube is a Google owned platform for hosting and sharing videos. YouTube collects user data through videos embedded in websites, which is aggregated with profile data from other Google services in order to display targeted advertising to web visitors across a broad range of their own and other websites.	Third Party	Targeting Cookies	youtube.com	Session

AWSALB	AWSALB cookies encodes information about the selected target, encrypts the cookie, and includes the cookie in the response to the client. It is required to manage Sticky session.	First party	Strictly Necessary Cookies	tcsempowers.tcsapps.com	Session
AWSALBTG	AWSALBTG cookies encodes information about the selected target, encrypts the cookie, and includes the cookie in the response to the client. It is required to manage Sticky session.	First party	Strictly Necessary Cookies	tcsempowers.tcsapps.com	Session
_cfuvid	This cookie is set when a site uses this option in a Rate Limiting Rule and to distinguish individual users who share the same IP address.	Third Party	Strictly Necessary Cookies	tcsempowers.tcsapps.com	Persistent
__cf_bm	This cookie is used to distinguish between humans and bots. This is beneficial for the website, in order to make valid reports on the use of their website.	Third Party	Strictly Necessary Cookies	tcsempowers.tcsapps.com	Persistent
_GRECAPTCHA	This cookie is set by Google as part of the reCAPTCHA functionality to provide spam protection and verify whether the data entry on our website is done by a human being or by an automated program	Third Party	Strictly Necessary Cookies	tcsempowers.tcsapps.com	Persistent

A cookie is a small piece of data (text file) that a website – when visited by a user – asks your browser to store on your device in order to remember information about you, such as your language preference or login information. Those cookies are set by us and called first-party cookies. More specifically, we use cookies and other tracking technologies for the following purposes:

We may periodically update this Cookie Policy to reflect changes in our practices. If needed, in such situations we will prompt you to revisit your cookie settings and submit your preferences again.

How to Control Cookies Manually

You can set your browser:

- To allow all cookies
- To allow only 'trusted' sites to send them
- To accept only those cookies from websites you are currently using.

We recommend not to block all cookies because TCS.com website uses them to work properly.

Please read below points to find out how to manage cookies in the major browsers.

Google Chrome:
Click on the "Menu" tab in the upper-right corner and then click on "Settings".

To block cookies:

Settings → Click on "Advanced" to expand → Under Privacy and Security, Click on "Content Settings" → Click on "Cookies" → To block cookies, Click on toggle button next to this line "Allow sites to save and read cookie data (recommended)" → This will block the cookies.

To check cookies:
Settings → Click on "Advanced" to expand → Under Privacy and Security → Click on "Content Settings" → Click on "Cookies" → See all cookies and site data → Click on the website and check the cookies used in that particular site.

Mozilla Firefox:
Click on the Menu tab in the upper-right corner → Click on Options → In the left side navigation, Click on Privacy and Security → Under History, Select "Use Custom setting for history" from the Drop down → Click on Show Cookies Buttons → Select the file which you want to remove and then click on remove selected button.

Internet Explorer:
Open Internet Explorer → Click on Tools menu in the upper-right corner → Click on Internet Options → This will open a window with many tab → Click on Privacy tab → Under Settings, move the slider to the top to block all cookies or to the bottom to allow all cookies → Then click Apply.

Open Internet Explorer → Click on Tools menu in the upper-right corner → Click on Internet Options → This will open a window with many tabs → Click on Privacy tab → Click on Sites button → Enter site name and then click Allow or Block button → If user clicks block button, that website is not allowed to use cookies in IE → Then click Apply.

Safari:
Open Safari → Click on Preferences from Safari menu → Go to Privacy tab → Click on "Remove all Website data" to remove all the stored data → Click Remove now button from the pop-up → Click on Details button under "Remove all Website data" → Select the sites you want to remove the data → Click Remove → Click Done.

To find information relating to other browsers, visit the browser developer's website.