DivorceMate Cloud (“DM Cloud”) Security Policy

Introduction

This Security Policy governs the processing of data provided by a Member in connection with DM Cloud. By using the Application, our services, or our website, you signify your acceptance of this policy. If you do not agree to this policy, please do not use our sites or DM Cloud.

There is a lot of legitimate concern about cyber-security with many malicious actors seeking to extract money using nefarious online methods.

While it might seem as if a server in your office with local PC’s is secure, if your inhouse network is connected to the Internet, it is incredibly vulnerable to attack, and Ransomware is typically placed on on-premise servers. Trojans often get placed on PC’s used for recreational purposes when we are least alert to danger.

Security on your PC is the responsibility of you and your IT provider. All information on your PC is vulnerable to attack without proper security precautions, so it is imperative to ensure every PC in your firm has the necessary anti-virus, malware and security protection.

Should your PC be compromised or lost, all your data on the DM Cloud servers would still be safe. All you need do is buy a new PC and login to DM Cloud. Your data will still be there.

The Microsoft Azure platform

Being a cloud solution, the software and all client data is stored on servers and services provisioned by the Microsoft Azure platform (“Azure”).

Azure is a leading cloud services platform, providing database storage, content delivery and a range of other functions. It is one of the largest and most successful cloud platform providers in the world.

Azure makes security its top priority, providing a data centre and network architecture built to meet the requirements of the most security-sensitive organisations. Azure is constantly evolving its core security services such as identity and access management, logging and monitoring, encryption and key management, network segmentation and Denial of Service (DDoS) protection.

Azure has an extensive and constant Cyber Security presence (its reputation depends on it) and DivorceMate routinely employs independent security experts to evaluate and continually enhance our security posture, implementing updates and patches in line with best practices.

Application data in DM Cloud is stored on Azure in Canadian data centres (Canada-Central & Canada-East regions) using SQL Database and CosmosDB. Active replication in SQL

Database ensures that the secondary data centre has an exact replica of data in the primary centre. Additional backups are also maintained by Azure. The principal application database has 35 days Point in Time Restore (PiTR) as well as additional retained backups. Time to restore is approximately 60 minutes.

Application Data

DivorceMate uses a multi-tenant architecture. Access to client-specific data is the responsibility of the client owner / administrator and handled through application authentication and authorization controls.

Application users authenticate using a username and password through a TLS encrypted interface (form-based login). The login form is protected by captcha and there is a limit on failed attempts before a user gets locked out and has to reset their password.

Application users can have ‘User’ and ‘Administrator’ claims, which expose different functionality in the application. An application user can have both claims. A ‘User’ can only access a subset of data / features (i.e. They have no ability to change organization data or add/remove users). An ‘Administrator’ has access to all organization data and can add/remove users. Data related to matters is only accessible by ‘Users’ and the application can be configured for matter privacy; under this scenario only ‘Users’ who are granted a claim to a specific matter have access.

Access to application data through the Azure portal and SQL Server Management Studio (SSMS) by DivorceMate employees is strictly controlled. Currently only 2 senior employees have access to the data stores. No other employee currently has access. Administrators of the Azure environment use a user ID and complex password, and IP-based restrictions are placed on Azure management interfaces. Only IPs belonging to DivorceMate are able to connect to the administrative interfaces.

TLS v1.2 encryption is used for transmission of all web traffic. TLS is a cryptographic protocol designed to protect information transmitted over the internet against eavesdropping, tampering, and message forgery.

The Azure SQL Database uses Transparent Data Encryption (TDE) at rest and uses an AES-256 encryption algorithm. Password hashes are stored in the database and are hashed using HMAC-SHA256.

Resiliency

DM Cloud has been designed to be a highly available SaaS solution. Servers are backed up in Azure multiple times daily, weekly and monthly. DM Cloud services are split over multiple Azure data centres within Canada. In the unlikely event that one data centre goes offline in a disaster scenario, the second data centre continues to serve data with minimal, if any, service interruption. DivorceMate is not responsible for any delays resulting from Azure server availability.

Third Party Security Consultants

We retain outside information security consultants specializing in application security testing to conduct comprehensive application vulnerability assessments (DASTs) and provide recommendations. The most recent report was prepared by cisphere.

Data Breach Notification

DivorceMate will notify the Subscriber without undue delay and in writing on becoming aware of any Data Breach in respect to our client's data.

If a vulnerability is identified or data is available publicly outside of the DivorceMate Software, please contact DivorceMate immediately via support@divorcemate.com.

Privacy Policy

DivorceMate's Privacy Policy is subject to change and can be accessed at: https://www.divorcemate.com/privacy.

DivorceMate and Your Data Security Responsibilities

Authorization

If you provide to DivorceMate any personal or sensitive data relating to other individuals, either directly, through our websites, through our software, or otherwise, you represent that you have the authority to do so and permit us to use, access, or host that data in accordance with this policy.

Account Access

DivorceMate employs industry standard security measures to ensure the security of information. However, the security of information transmitted through the Internet can never be guaranteed. DivorceMate is not responsible for any interception or interruption of any communications through the Internet or for changes to or losses of information. Site users are responsible for maintaining the security of any password, user ID, or other form of authentication involved in obtaining access to password protected or secure areas of any DivorceMate websites or applications.

In order to protect you and your information, DivorceMate may suspend your use of a website, without notice, pending an investigation, if any breach of security is suspected. Access to and use of password protected and/or secure area of any unauthorised access to such areas is prohibited and may lead to criminal prosecution. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any account you might have with us has been compromised), please immediately notify us of the problem by contacting us in accordance with the "Contacting Us" section herein.

As more fully detailed in DivorceMate’s Privacy Policy, we may use your information as we believe to be necessary or appropriate:

1. under applicable law, including laws outside your country of residence;
2. to comply with legal process;
3. to respond to requests from public and government authorities including public and government authorities outside your country of residence;
4. to enforce our terms and conditions;
5. to service providers which act for us or provide services for us, such as for marketing or for the processing of payments, and as to such service providers their use of Personal Information is subject to our agreements with them and any applicable laws;
6. to protect our operations or those of any of our affiliates;
7. to protect our rights, privacy, safety or property, and/or that of our affiliates, you or others; and
8. to allow us to pursue available remedies or limit the damages that we may sustain

Questions?

This statement reflects the security policy of DivorceMate and is regularly reviewed and updated. It should be regarded as the primary source of truth regarding security within DivorceMate. Any questions should be directed to support@divorcemate.com.

Last Updated: 30 September 2022