Security

It is an important fact in today's hi-tech world that certain auditory and visual information converted into digital form and stored in a database system such as SUNRISE Contacts 2020 and can be accessed quickly and easily by people need to be secure. In fact, there are strict state and federal privacy regulations governing the security of people's personal and business confidential information held in any centralized electronic storage system.

To make SUNRISE Contacts 2020 secure for organizations, please keep in mind the following:

1. SUNRISE Contacts 2020 is designed to protect your data
We have designed SUNRISE Contacts 2020 to give you the peace of mind of knowing your information will not be surreptitiously sent to a third-party without your consent. We value your privacy, so you can be assured we are not here to monitor what you do with this product, or the data contained therein. This is your product. Use it as you like in any way you think is best.

2. Sending encrypted emails
Always configure your email-sending application to encrypt emails before sending them over the network. Encryption makes it extremely difficult for anyone on the network to recognize them as part of your emails and know precisely what is in them. Even if someone else is able to know you were sending emails and could intercept and capture all the relevant packets of information, it will take considerable time (if not impossible) to decipher the encryption depending on how strong the encryption algorithm had been in the first place, by which time hopefully the emails will become redundant or irrelevant. Always use the best encryption offered by your preferred email-sending application or plug-in. In SUNRISE Contacts 2020, there is an option to select encryption in the Email Setup layout - namely, SSL (the standard) or TLS encryption. Otherwise, it is strongly recommended that you go into the email-sending application directly, and select the available encryption level you want from the Preferences section (always check with your ISP to make sure the encryption service is supported). Then you should be safe (well, a lot safer than the unencrypted form).

3. Web published data transferred between the web page and the database must be encrypted
Always establish an *https* (or better still a proxy server known as a PPTP) encryption (and anonymity) service for data being sent between SUNRISE Contacts 2020 on the server and a web browser (for example, if you choose to access the data of your database(s) in web publishing mode using FileMaker Server/Cloud and WebDirect or PHP/XML/REST). And also ensure people who are entitled to access the web published database data must do so by entering a username/password on the web page. Talk to

your ICT manager about establishing an *https* (or PPTP) service. Also the server providing you with access to the database data should always be located within your organization (not a third-party server hosted outside your organization by someone you don't know unless the information is not sensitive). And as an added security measure, establish a point-to-point proxy connection between you and the server. A Virtual Private Network (VPN) is an example of a proxy. This type of connection is considered even more secure than using SSL because not only is the data encrypted, but people will never be able to see the metadata headers. The entire encrypted data will appear as static noise to anyone who tries to listen in on the connection. Furthermore, a VPN effectively strips the originating IP address, making it anonymous. In other words, your IP address will not be shown to anyone, only the IP address of the proxy server, thereby adding yet another level of security. Once a secure server is established, you will be provided with a secure web address by your ICT manager for you to access SUNRISE Contacts 2020 via a web browser on your preferred device.

4. PDF files sent by FTP should be encrypted

When printing PDF files of any sensitive record or data within SUNRISE Contacts 2020 and later sent electronically to other people on the network using the file transfer protocol (FTP) method, make sure the FTP application you use to send the files is set up to encrypt the files. Talk to your ICT manager for further information about how to do this. Also consider putting a password on the PDF file you have created. Please note that this password method is not perfect — Adobe doesn't properly encrypt the entire PDF file as they need to access data (especially in the metadata header) to see if you are using a legitimate copy of any Adobe application and, if not, to identify you by reading the metadata header and/or the contents of your PDF. Because the encryption quality is a little underwhelming from Adobe, there are tools available to unlock just about any PDF file in existence. Despite this, the provision of a basic password authentication system to access your PDF will still provide some level of deterrent for most other users not familiar with techniques to unlock your PDF.

5. Minimize the number of staff accessing the more sensitive data and always keep staff happy

The biggest cause for data breaches is disgruntled employees. We recommend that you look after the employees (and probably pay them well) and keep the number of staff who need to access sensitive information to an absolute minimum. A hierarchical structure in authentication accounts should be established where only a few trusted staff members with sufficiently high privileges can access more sensitive and a wider range of data, and more staff with lesser privileges may access less sensitive and a restricted range of data. In SUNRISE Contacts 2020, there should be only one or two people who have Owner access privileges (usually the people who purchased the database or manager of the organization), a few more people having Admin access privileges, and the rest having Guest access. SUNRISE Contacts 2020 provides an Access layout through the File menu (look for "Access…" to control access to selected databases based on user accounts, and establish new accounts

through Manager→Accounts as you see fit). Use it to control all the access you need to selected users. Also when setting up the databases on the network, make sure the databases that need access by users are visible and that every other database is kept invisible in FileMaker Server/Cloud. This latter approach provides you with yet another layer of excellent security measures.

6. Avoid copying or exporting sensitive data and storing it on any portable storage device.
A USB memory stick may be enormously convenient for carrying digital information with you in a highly compact means, but it is a terrible form of security should you lose the stick. Always work from the original data source (i.e., SUNRISE Contacts 2020) kept on a secure server (i.e., the computer within your organization delivering the databases). When working from the original source via a web browser, make sure you have a secure online address to this source (i.e., at least an https type of connection, or better still go for a proxy server), and use an iPad or similar viewing device (but don't store information from the source on it). If, heaven forbid, you should ever lose the iPad or other portable device, at least the data and database remain secure and safe on another storage device, and confidentiality of the information is maintained. Provide staff with portable web access devices, such as an iPad, to help them access the data anywhere they like. Inform staff not to store usernames and passwords on their iPads or anywhere else.

7. Minimize the use of online services that request a unique API key when accessing their data.
While we incorporate Google Maps, PayPal invoice creation, and the ability to download currency rates whose data is supplied by online services, you will notice that more and more of these services are moving towards a "pay-as-you-use" model. This means that you may be required to get your own API key as well as supply your financial details as a means of paying for the service, or at the very least identify who you are. The problem with this approach is that the key is a powerful tool to identifying who you are, what data you are grabbing, and hence who you communicate with, the places you visit, and how much you are receiving by way of income and other things. This is a security problem, and a potential breach of your privacy if these services are not properly securing this data collected from you. As a result, we will download as much of the critical data you are likely to need from various free sources and keep them permanently available in its own lookup databases. For Google Maps, we have included in version 4.1.5 and above of SUNRISE Contacts the ability to switch to OpenStreetMaps (a free service). Just go into the contacts details card layout, and press Shift Option Ctrl keys as you click the world icon in the addresses for a dialog box to appear. From there you can switch to a different map service. The critical thing is, if you can access the service online without an API key, there is no security issues to worry about other than the fact that you will be advertising your IP address and the ISP who you are with (a VPN service provider can help in this regard). Then you can access the data freely without any further costs or needing to have an online account and API key. For changeable data, such as currency rates, we will choose the best free online services and reduce how often you

access this data to ensure the services remain free. Beyond that, you must choose whether to grab an API key or not. If you need to have one, there will be a place in SUNRISE Contacts to store it (and it may open up additional new services if security and privacy is not too much an issue for your business and personal use).

8. Clear HDD storage media in printers
Most high-end printers will have the option to store documents on an internal hard drive or nearby Fiery server and this tends to be accessible on a network. Strictly speaking, the storage space previously reserved temporarily to print a document should be cleared from the hard drive properly. However, most older printers do not security clear the space. If you have Administrator privileges, you should go into Admin mode and set the System timers to clear the hard drive every day, if not more regularly as is practical. Indeed, the latest Ricoh printers will now overwrite the space temporarily held for a document with random sequences of "1's" and "0's" immediately after the document has been printed and sees it as a standard approach. Also, if the hard drive is ever removed without authorization and with the slightest possibility of retrieving the document through file recovery software, each document sent to the hard drive is encrypted. With security now on the minds of more and more companies, expect printer manufacturers, such as Fuji-Xerox and others, to quickly jump on this "security" bandwagon and release the latest breed of more secure printers, including digitally-signed firmware updates for that extra level of protection.

9. Backups of SUNRISE Contacts 2020 should be encrypted
Always keep a backup copy of SUNRISE Contacts 2020 with any sensitive data it contains on a separate backup disk (not accessible on the internet) and it should be encrypted. One way to achieve this is by creating a .dmg file (for Mac users) or .zip (for PC users) setup with at least 256-bit encryption and password (this is considered the basic level for all commercial purposes, but not military-grade unfortunately). Use Apple's Disk Utility to create the encrypted .dmg file. For PC users, there should be a number of better quality ZIP compression apps with encryption capabilities.

For Mac users who create a .dmg file (make sure it is large enough to hold all the databases), you can backup SUNRISE Contacts 2020 as follows:

1. Open the .dmg file. A virtual disk icon will appear on the desktop.
2. Open the virtual disk icon.
3. Transfer a copy of SUNRISE Contacts 2020 to the virtual disk.
4. After copying, eject the virtual disk. The database will be stored and encrypted inside the .dmg file.
5. Copy this .dmg file to a backup disk. Make at least two backup copies (preferably on different backup disks) for organizations serious about protecting their data.
6. Establish a regular regime of backing up your data, either daily, weekly or monthly, depending on the importance of your information.