



Security and Risk Management

2012-05-15

Disclaimer

THIS DOCUMENT WAS PREPARED TO HELP USERS OF SOFTWARE OF SOFTWOOD TECHNOLOGY INC. (“SOFTWOOD”). THE CONTENTS OF THIS DOCUMENT SHALL NOT BE USED FOR ANY OTHER PURPOSE WITHOUT THE EXPRESS WRITTEN PERMISSION OF SOFTWOOD. SOFTWOOD SUPPLIES THE MATERIAL IN THIS DOCUMENT AS IS, WITHOUT CONDITION, REPRESENTATION OR WARRANTY, EXPRESSED OR IMPLIED, OF ANY KIND. SPECIFICALLY, SOFTWOOD DISCLAIMS AND EXCLUDES ANY CONDITION OR WARRANTY, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY AND DISCLAIMS AND EXCLUDES ANY CONDITION OR WARRANTY, INCLUDING ANY IMPLIED WARRANTY, OF FITNESS. THERE ARE NO WARRANTIES WHICH EXTEND BEYOND THE DESCRIPTION ON THE FACE HEREOF.

Trademarks

Throughout this document, certain designations may be used that are trademarks that identify the goods of third parties. Although this document attempts to identify the particular trademark owner of each mark used, the absence of a trademark symbol or other notations should not be taken as an indication that any such mark is not registered or proprietary to a third party. Use of such third-party trademarks is solely for the purpose of accurately identifying the goods of such third party.

Softwood, Sumac, and the Sumac logo, are trademarks of Softwood Technology Inc.

Copyright

Copyright © 2011,2012 Softwood Technology Inc.

All rights reserved. Reproduction of this document or any portion of it, in any form, without the express written consent of Softwood Technology Inc. is prohibited.

Table of Contents

Disclaimer – 2	
Trademarks – 2	
Copyright – 2	
Sumac Documentation – 5	
Introduction – 6	
Overview – 6	
PCI DSS – 6	
Relationship With Developer – 7	
Confidential Data Handling – 7	
Is Data Lost When A New Release of Sumac Occurs? – 7	
Access To Database – Passwords – 8	
Introduction – 8	
Database User IDs and Passwords – 9	
Sumac User IDs and Passwords – 11	
Password Obfuscation – 11	
Password Aging – 12	
Password Quality – 12	
Database Hosting – Sumac Online – 13	
Visibility of Data in Sumac – 14	
Overview – 14	
Access By Data Types – 14	
Contact Segments – 15	
User Profiles – 15	
Sensitive Contacts and Communications – 17	
Extra Fields – 17	
Multiple Databases – 18	
Key Records – 19	
Special Warning – 19	
Introduction – 19	
Approach Taken – 19	
Initial Set-up – 21	
Create a New Key Record – 23	
Delete Key Records – 24	
Additional Security Features of Sumac – 26	
Preferences Command – Security Tab – 26	
Backing Up Your Database – 27	
Website Encryption – 27	
Retention Period Policy – 29	
Introduction – 29	
Establish a Retention Period (RP) – 29	
Delete Old Backup Databases – 29	
Payment Information in the Sumac Database – 29	
Key Management – 29	
Payment Processing Security in Sumac – 30	
Introduction – 30	
Summary – 30	
Supported Operating Systems – 30	
Target Industry and Customers – 30	

Support Connections to External Processors and Card Brands – 30
Typical Implementation – 30
Data Storage Locations – 31
Versioning Methodology – 31
Do not retain full magnetic stripe, card validation code, or PIN block data – 32

PCI DSS Compliance – 34

Introduction – 34
Build and Maintain a Secure Network – 34
Requirement 1: Install and maintain a firewall to protect cardholder data – 34
Requirement 2: Do not use vendor-supplied defaults for system passwords – 35
Protect Cardholder Data – 36
Requirement 3: Protect stored cardholder data – 36
Requirement 4: Encrypt transmission of cardholder data across open networks – 37
Maintain a Vulnerability Management Program – 37
Requirement 5: Use and regularly update anti-virus software or programs – 38
Requirement 6: Develop and maintain secure systems and applications – 38
Implement Strong Access Control Measures – 39
Requirement 7: Restrict access to cardholder data by business need to know – 39
Requirement 8: Assign a unique ID to each person with computer access – 39
Requirement 9: Restrict physical access to cardholder data – 41
Regularly Monitor and Test Networks – 42
Requirement 10: Track all access to network resources and cardholder data – 42
Requirement 11: Regularly test security systems and processes – 43
Maintain an Information Security Policy – 44
Requirement 12: Maintain a policy addressing information security for all personnel – 44

Sumac Documentation

Sumac is described in three books:

<i>Sumac Users Guide</i>	Use Sumac on a day-to-day basis.
<i>Sumac Administrator Manual</i>	Install Sumac. Set up system-wide lists and options settings that affect all users.
<i>Security and Risk Management</i>	Use Sumac to protect your data.

Introduction

Overview

Security is a broad topic. It usually entails getting good answers to questions like this:

- Can I get my data out of Sumac?
- Will my confidential data be handled properly?
- What if a computer fails?
- Can people steal my data?

What these questions have in common is the management of risk. When you start to use Sumac, you are investing effort in converting your data, training your staff, and creating a valuable data resource on which your organization will be dependent. You want to ensure that this effort is protected from attackers and preserved over time.

This document addresses these questions and many others. If there is a missing topic that you think should be addressed in this document, please let us know.

PCI DSS

If your installation of Sumac stores and processes payment information, then your organization must comply with *PCI DSS* – a standard for ensuring the secure handling of payment information.

Specific information about this standard appears in the chapter *PCI DSS Compliance* at page 34.

In addition, some parts of this manual describe how to use certain features of Sumac which are important to ensuring that your management of data complies with PCI DSS. These parts of the manual contain warnings that look like this:

Warning: In order to comply with PCI DSS you must use the feature of Sumac that is described in this section of the manual.

Relationship With Developer

Confidential Data Handling

We are very careful with your data. Our standard contracts require confidentiality in the handling of data. You can read these terms here:

<http://sumac.com/documentation/StandardTerms2010-08-03.pdf>

Occasionally we have comforted a customer's lawyers by signing their standard confidentiality agreement. We can do this for you too.

Is Data Lost When A New Release of Sumac Occurs?

The most recent release of Sumac is available without additional charge to every Sumac user. We expect all our customers to be using the most recent release at all times.

If there is a change to the structure of the database, Sumac does this for you automatically. No data is ever lost.

Access To Database – Passwords

Introduction

DBMS

Sumac stores its data in a database. A database is a collection of files, usually called tables, of related information.

A database is managed by a database management system (DBMS). A DBMS is a piece of software that accepts requests to add, change, or remove data from a database.

Sumac can work with any DBMS, if configured appropriately. But usually it works with these databases:

- ◆ JavaDB: a single-user DBMS used by Sumac Bronze and Sumac Silver
- ◆ MySQL: a multi-user DBMS used by Sumac Gold. MySQL is also used by Sumac Bronze and Sumac Silver if they are used in conjunction with Sumac Online.

Database User ID and Password

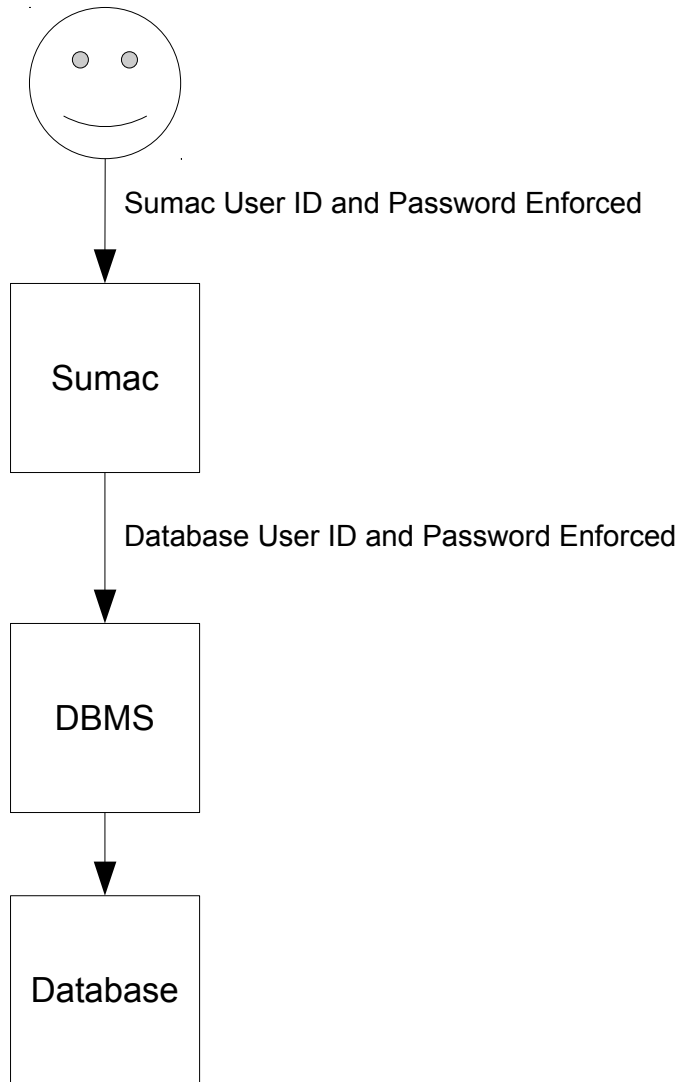
A DBMS requires a user ID and password when Sumac initially connects to a database. These are managed by tools associated with the DBMS.

Sumac User ID and Password

Each user of Sumac has a user ID and password. These indicate what the user is allowed to do with various types of data in the database. Sumac user IDs and passwords are managed by the Users command in the Administrator menu in Sumac.

Diagram

The following diagram shows how these pieces fit together:



Database User IDs and Passwords

JavaDB – Single-user Databases

Sumac Bronze and Sumac Silver databases are single-user databases. For single-user (JavaDB) databases, you cannot change the database user ID and password. Since a single user database is stored entirely on the computer that uses it, it cannot be accessed remotely by Sumac. It relies on operating system access to the computer to protect access to the database.

MySQL – Multi-user Databases

Sumac Gold databases are multi-user databases. Sumac Bronze and Sumac Silver databases are also multi-user databases when they use the Sumac Online service.

Multi-user Sumac databases use MySQL – a DBMS – to hold the data. A standard installation of Sumac on MySQL within a single organization's office uses a standard database user ID and password. If your MySQL database is only acces-

sible from within your office, then there is no need to change this user ID and password. However, if your office network and database can be accessed remotely, then you should change the database user ID and password.

When you use Sumac Online, we take care of this issue for you: the database is protected by a long randomly generated database user ID and password. We configure the DBMS and tell you the database user ID and password to use to connect to your database.

If you do not use Sumac Online, then to make this change, you need to configure the DBMS to recognize the new user ID, and you also need to tell Sumac the user ID and password that it needs to use to connect to the DBMS. Here is what to do:

Create User On Server

- ✓ On the server computer, run MySQL Workbench.
- ✓ Log on as administrative user.
- ✓ Click Manage Security, and choose the server.
- ✓ Under Server Access Administration, specify the new database user ID and password.
- ✓ Click Apply. This gives the new user ID the ability to connect to the DBMS.
- ✓ Click Schema Privileges
- ✓ Click the default user (cfrUser). Click to select all rows of security information for that user, then click Delete Entry. This removes all access to the database by the default user ID.
- ✓ Click to choose the newly-added database user ID and password, then click Add Entry.
- ✓ Click Selected Schema, then click to choose your database, and click OK.
- ✓ Click Select All to give the new database user ID and password all privileges on your database.
- ✓ Click Save Changes.

Tell Sumac How To Connect

When Sumac starts, it determines which databases it can access by looking at the databases.txt file. This file is stored in the user's home directory in a folder named SumacSettings.

Each line in this file represents a different database that Sumac can connect to. Each line contains two or four pieces of information, separated by spaces.

<i>Parameter</i>	<i>Example</i>
database connection string	<code>jdbc:mysql://DBServer/MyDbName</code>
driver class name	<code>com.mysql.jdbc.Driver</code>
database user ID	<code>newDbUserID</code>
database password	<code>newDbUserPassword</code>

If the examples in the above table were used, then the line in the databases.txt file would look like this (all on one line):

```
jdbc:mysql://DBServer/MyDbName com.mysql.jdbc.Driver newDbUserID  
newDbUserPassword
```

Sumac User IDs and Passwords

Warning: You must remove default user IDs and passwords to conform with the PCI DSS standard for handling payment data.

Default User ID

When you first install a Sumac database, it has only a single user ID and password: *admin* and *admin*.

If you have a single-user database, *and* it cannot be accessed remotely, *and* you do not process payments, then there is no security reason for changing this. However, even in this restricted situation, you may still want to change it to reflect the actual user name(s) of the user(s) entering data into the database, since Sumac tracks this, and it is useful to know which user recorded information, especially communication information, in the database.

Setting Up Proper User IDs

If you use Sumac to handle payment information, then the first thing you must do when you get a new Sumac database is to define a user and give the user Administrator capability, then remove the default *admin* user account. Here is what to do:

- ✓ Log on with the admin user account.
- ✓ Choose the Users command from the Administrator menu.
- ✓ Click New to add a new user, specify the user's name and password, and ensure that you give the new user Administrator privileges.
- ✓ Quit Sumac. Run Sumac and log on with the new user ID.
- ✓ Make sure the new User ID has access to the Administrator menu.
- ✓ Delete the default *admin* account

You add and change Sumac users as follows:

- ✓ Log on to Sumac as an administrative user.
- ✓ Choose the Users command from the Administrator menu.
- ✓ Add, remove, and edit users as required.

Password Obfuscation

Warning: You must use password obfuscation to conform with the PCI DSS standard for handling payment data.

When you add new users to your Sumac database, a record is stored in the database. This record holds the Sumac user ID and password for the user, and also indicates what each user is allowed to do to each type of data in the Sumac database. The passwords stored in the database are stored as regular text.

This has the advantage that it makes password recovery possible with fairly simple technical tools. However, this approach also causes a security issue by making it easier for a skilled attacker to hack into the database.

Password Obfuscation is used to prevent Sumac from saving passwords as regular text. Instead, the passwords are saved as hashed¹ text.

To turn on password obfuscation in Sumac:

- ✓ Log on to Sumac as an administrative user.
- ✓ Choose the Preferences command from the Administrator menu.
- ✓ Click in to the Security tab.
- ✓ Click to set the *Obfuscate Passwords* checkbox.

¹ SHA-256

- ✓ Click OK to save the change.

Password Aging

Warning: You must use password aging to conform with the PCI DSS standard for handling payment data.

Sumac supports password aging. Password aging is a security feature that forces users who can see payment information to change their password every 80 days. It also prevents a user from using a password that has been used before: Sumac keeps track of the last five passwords that a user has used.

To turn on password aging in Sumac:

- ✓ Log on to Sumac as an administrative user.
- ✓ Choose the Preferences command from the Administrator menu.
- ✓ Click in to the Security tab.
- ✓ Click to set the *Age Passwords* checkbox.
- ✓ Click OK to save the change.

Password Quality

Hint: High quality passwords are needed to conform with the PCI DSS standard for handling payment data. Sumac enforces this automatically and you cannot turn off this feature.

You need to be able to log in as a user in order to use Sumac. This requires you to enter a user ID and a password. Any string of characters can be used as a password, but since these passwords provide protection for your data, it is unwise to use something like your name or a simple string of characters (e.g. *1234*).

If you have trouble thinking up a good password, when you are entering the password for a new user, Sumac can suggest high quality passwords generated randomly from alphabetic, numeric, and special characters.

Specify the User Password

Password

Password (confirm)

If the user is an administrator or can see payment records, the password must:

- contain at least one alphabetic character (A to Z, a to z)
- contain at least one numeric character (0 to 9)
- contain at least one character that is not alphabetic or numeric
- not contain spaces
- be at least 7 characters long

If a Sumac user is going to be an administrator or will be able to see payment details, then the user's password must be better quality. It must satisfy the following criteria:

- ◆ contain at least one alphabetic character (A to Z, a to z)
- ◆ contain at least one numeric character (0 to 9)
- ◆ contain at least one character that is not alphabetic or numeric
- ◆ not contain spaces
- ◆ be at least 7 characters long

As you type each character into the first password field, Sumac indicates exactly which of the above criteria are and are not satisfied.

Database Hosting – Sumac Online

If you use Sumac Online, our database hosting service, your database user ID and password were set for you by Sumac staff. Both the user ID and the password are long, randomly-generated alphanumeric strings. We never store these passwords electronically, except briefly when a *picture* of them is emailed to you.

The database user ID and password provide additional security, protecting databases from remote access, but Sumac user passwords are still very important.

Part of your Sumac Online service is daily backups. These backups are encrypted so even if the computer on which they reside is stolen, they are still not accessible without additional passwords to provide access to the decryption.

Daily backups are retained for one month, and monthly backups (the last of each month) are retained for six months.

Visibility of Data in Sumac

Overview

Once you are logged on to Sumac, what can you see? What can you change? What can you delete? Sumac provides several ways that you can configure the database to ensure that each user sees only the data he or she is supposed to see.

Access By Data Types

Sumac requires you to create a user profile for each user who is allowed to use the database. This profile indicates what types of data the user is allowed to see (View), to change (Edit), and to remove (Delete).

Data or Commands	View	Edit	Delete	Special
Auctions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Campaigns	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Collections	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Communications	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Contacts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Course Registrations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Donations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Fund Programs and	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Job Openings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Pledges	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Payments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Sales	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Proposals	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Prospect Ratings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Reminders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Submissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Memberships	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Subsidiaries	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Ticket Orders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Contact Segments
Set checkboxes for segments of contacts the user may view.
If the user can see all segments, do not set any checkboxes.

Fundraising Patient Student

OK Cancel

Contact Segments

Sumac allows you to put each contact in the database into a segment. You can define as many segments as you want.

Users are only allowed to see contacts, and data related to them, if they are authorized to see the particular segment.

For example, the picture above shows that the database is divided into three segments: Fundraising, Patient, and Student data. When a user is defined, you can indicate that the user is allowed to see contact records that are in one, two, or all three of these segments. The following table shows what a user is allowed to do and see in a segmented database:

<i>Segments User Sees</i>	<i>Contacts the user can see</i>	<i>Can user move contacts between segments</i>
All segments	The user can see all contacts including those that have not been assigned to a segment.	The user can move a contact from one segment to another, including putting a contact in no segment at all.
One segment	The user sees only contacts in the one segment.	The user is unaware of the presence of the other segments, and cannot move contacts between segments.
More than one but not all	The user can see contacts only in the specified segments.	The user can move contacts between the segments he is allowed to see.

User Profiles

Every Sumac user needs to log on to Sumac using a user ID and password. These are defined by a Sumac administrator using the Users command in the Utilities menu.

In the user profile, you use checkboxes to indicate what types of data a user is allowed to see, change, and delete.

In addition, at the bottom of the list of checkboxes for viewing, editing, and deleting data, there are some special checkboxes.

<i>Checkbox</i>	<i>Function</i>
Administrator	This checkbox indicates that this user is a Sumac administrator, and so should have access to the commands in the Administrator menu.
Bulk Import	This checkbox allows the user to use the Import command in the Utilities menu and also to use Set Values buttons.
Adjust Order Pricing	This gives the user the ability to adjust the pricing of ticket and sales orders.
Ticket Holds	This lets the user hold (reserve) seats for a particular event.

<i>Checkbox</i>	<i>Function</i>
Sensitive Data	This lets the user mark contact and communication records as being sensitive. It also allows the user to see contact and communication records that have been marked as sensitive.

User

Login Name

Notes

Accepts Licence

Locked (log-on is prevented)

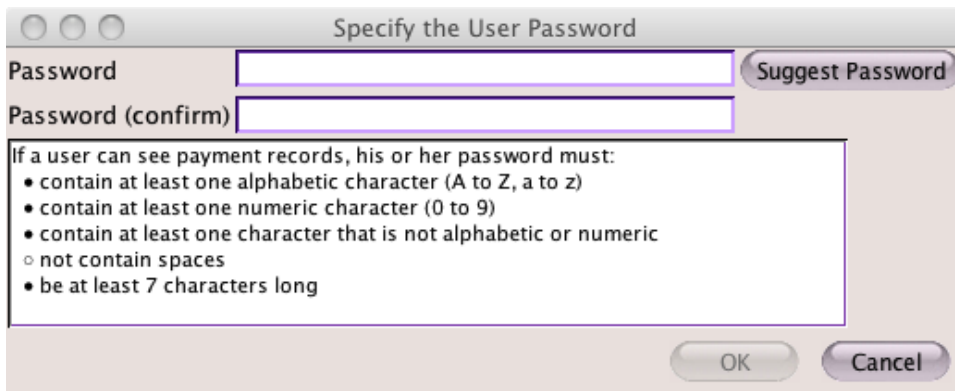
Data or Commands	View	Edit	Delete	Special
Payments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Sales	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Proposals	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Prospect Ratings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Reminders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Submissions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Memberships	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Subsidiaries	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Ticket Orders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Tour Bookings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Bookings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Thingies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Time Dockets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Administrator				<input type="checkbox"/>
Bulk Import				<input type="checkbox"/>
Adjust Order Pricing				<input type="checkbox"/>
Ticket Holds				<input type="checkbox"/>
Receive Email				<input type="checkbox"/>
Sensitive Data				<input type="checkbox"/>

Contact Segments

Set checkboxes for segments of contacts the user may view.
If the user can see all segments, do not set any checkboxes.

Fundraising Patient Student

You must set a password for each user. Click the Set Password button to see this dialog:



Anything can be used as a password, but if the user is allowed to see payment information, then the password must be stronger. It must satisfy all the requirements listed in the text box in the dialog. As you type a password in the first field, the circles in front of each requirement become empty circles if the requirement is satisfied, and filled-in circles if the requirement is not met. When all the circles are empty, the password is good enough to allow the user to see payment information.

Sensitive Contacts and Communications

Sumac allows you to divide your users into two groups: those who can see sensitive data and those who cannot. Users who can see sensitive data are also allowed to mark contacts and communications as sensitive. The *User Profiles* section on page 15 describes the Sensitive Data checkbox which gives users the ability to see sensitive data.

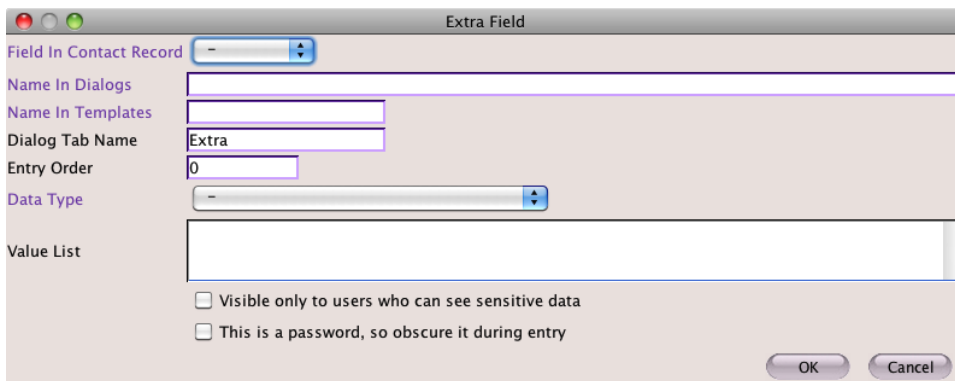
If a communication record is marked as sensitive, a user who cannot see sensitive data will not be allowed to see the communication or even to know that it exists.

If a contact record is marked as sensitive, a user who cannot see sensitive data will be able to see only the contact's name; any other details will not be displayed in the contact's list. Also, when the user double clicks to edit a contact, he will be told he is not allowed to see or edit a sensitive contact.

Extra Fields

Contact records come with hundreds of pre-defined fields of data. But you can extend the data stored about each contact by defining additional extra fields. These extra fields are placed on extra tabs in the user interface of the dialog which displays contact information in Sumac.

Here is the dialog used to define an extra field:



You can click *Visible only to users who can see sensitive data* to ensure that only users authorized to see sensitive data can see this field. See *Sensitive Contacts and Communications* on page 17.

If the field holds a password, perhaps one that is entered by members who use your website, click *This is a password, so obscure it during entry*. This checkbox causes the text in the field to be obscured, showing only bullets instead of the actual characters in the field.

Multiple Databases

Sumac has a Multiple Databases feature. This allows you to set up several databases, perhaps one for each of several related organizations. You can then define user access to the database. Since each organization has a completely separate database, users of one do not see the contents of the other.

Key Records

Warning: In order to comply with the PCI DSS requirements, you *must* create and manage keys as described in this chapter.

Special Warning

When creating and deleting Key Records, you should ensure that no other users are currently using Sumac. This ensures consistency of the encryption of payment information.

Introduction

When you save payment information into the database, some things like the ID of the payer (a contact record in Sumac), and the amount of the payment are saved as regular database fields. This is fine for this type of information, which would not be useful to a thief trying to steal credit card information. But this is not an acceptable way to save credit card information (card number, expiry date, etc.) because someone with evil intentions might monitor database or network traffic and be able to figure out credit card details.

So credit card information is *encrypted* when it is put into the database. This means that it is converted into a very large number which then has some mathematical transformations done to it so that it no longer looks like what it is. Sumac is able to encrypt the card information, turning it into an obscure large number, and is also able to *decrypt*, which reverses the process and turns the obscure large number back into credit card information.

If you let Sumac operate in its default way, it will use encryption and decryption that work the same on all Sumac databases. This is certainly better than just saving the data into the database without encryption, and it is a huge improvement over saving the data in a spreadsheet or word processing document, but it is still not as good as it could be, and it is also not good enough to satisfy the PCI DSS requirements.

To enhance the security of stored payment data even further, and to comply with the PCI DSS requirements, you need to specify encryption that is specific to your own organization. This chapter explains how use Sumac to achieve this higher level of security.

Approach Taken

Public and Private Keys

As payment records are created, the credit card details in the payments are encrypted and decrypted with keys². These keys come in two parts: a *public key* and a *private key*. The public key is used to encrypt (protect) payment information, converting it into a form that cannot be interpreted. The private key is used to decrypt the encrypted data, converting it back into an understandable format.

Public and private keys come in pairs. Each public key can work only with its corresponding private key and vice versa. One way to think of this is that the public key is used to lock the data so it cannot be used, while the private key is used to unlock it and open it up for usage.

As the names would suggest, the public key does not need to be protected too carefully: it can be exposed to the public. Since it is used to encrypt data, some-

² 256-bit RSA

one using it must already have the data that is being protected, so having access to the public key does not provide any additional information.

In contrast, the private key must be protected. Someone with the private key can decrypt and examine any data that was encrypted (protected) by the corresponding public key.

In the Sumac database, credit card information is protected by encrypting it with a public key then, when it needs to be used, decrypting it with the corresponding private key.

Key Records in Sumac

In Sumac a Key Record holds a public and private key pair that can be used to encrypt and decrypt credit card payment information. A Key Record contains the following fields:

<i>Field</i>	<i>Content</i>
ID	An internally assigned ID that ensures the key is unique within the database.
Effective Date	This date should be set to the date when the keys are created. All Key Records with the same Effective Date contain the same Public Key and Private Key. When a payment is encrypted using the public key of a particular Key Record, the Effective Date of the Key Record is put into the payment. Later, when Sumac needs to decrypt the payment, it uses the Effective Date (stored as part of the payment record) to find the correct Key Record – the one which contains the Private Key that can be used to decrypt the payment.
User ID	The ID of a Sumac user. When a user logs on to Sumac, he or she must enter a Sumac User ID and Password (see page 11). As soon as the Sumac User ID and Password are validated and the user is logged on to the Sumac database, the user will be asked to enter the Password (see next field) for each Key Record that contains that user's ID. This ensures that as Sumac encounters encrypted payment information, it will be able to decrypt it and show it to the user who is logging on.
Password	This field in the database does not actually contain the user's password. Instead, it contains a hash ³ of the user's password. A hash is a large number which is computed from the password. Someone knowing the hash cannot figure out what the password is, however if a user enters the password, Sumac can compute its hash and determine if the correct password has been entered. This enables Sumac to know if a user knows the right password without actually storing the password in the database.

³ SHA-256

<i>Field</i>	<i>Content</i>
Public Key	This is the RSA public key, used to encrypt payment information. When Sumac needs to protect payment information (the credit card details in payment records), it looks at the entire list of Key Records, finds the one with the highest effective date, and uses the public key in that Key Record to encrypt the information.
Private Key	This is the private key that is needed to decrypt credit card information that was encrypted using the Public Key in this Key Record. The Private Key, as stored in the Sumac database, is encrypted ⁴ using the password for the user of this Key Record.

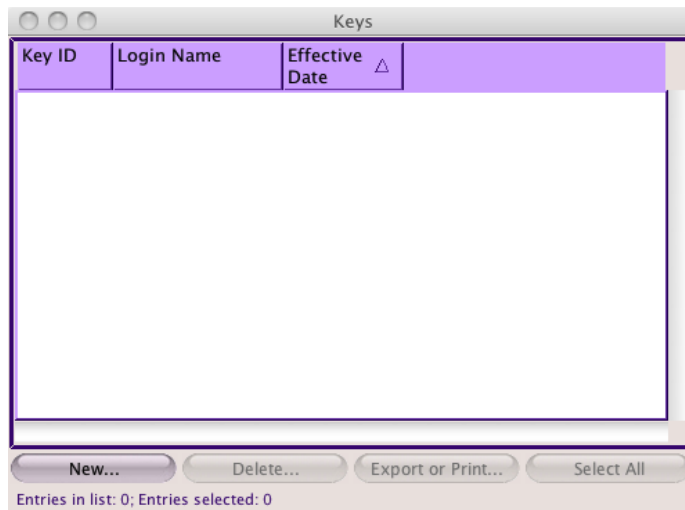
Initial Set-up

As soon as you create a Key Record, Sumac will start using it to encrypt new payments as they are entered into the database.

Create the First Key

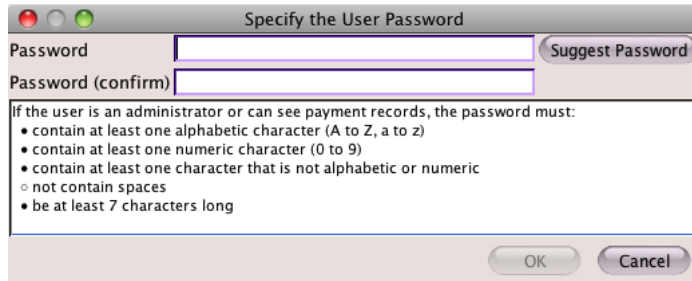
Here is how to create the very first Key Record:

- ✓ Log on to Sumac as an administrative user.
- ✓ Choose the Keys command from the Administrator menu.



- ✓ Click the New button. This first key will be created with your User ID. You are asked for a password. This password is to protect the private key in the Key Record being created. Note that it does not need to be the same as the password that you use to log on to Sumac, nor does it need to be the same as any other key that you may use to protect other Key Records. The password does, however, need to be one that is sufficient to protect payment records. As you enter characters in the password, the black circles in front of the password requirements become hollow as your password satisfies each criterion. You must satisfy all the requirements.

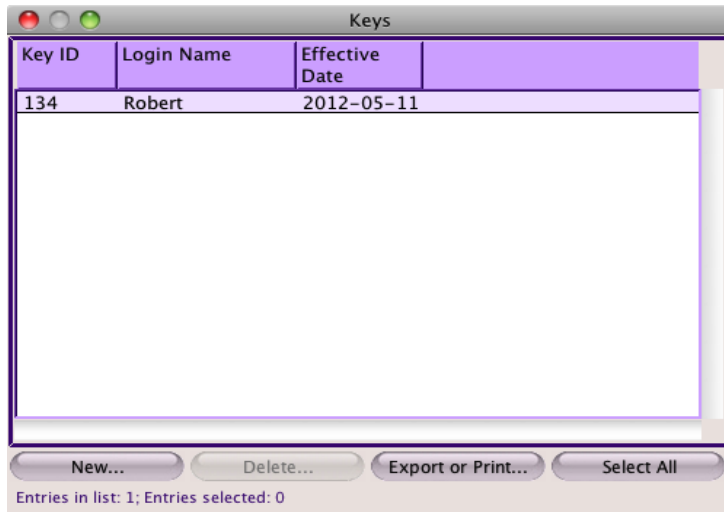
⁴ triple-DES



- ✓ Once you have specified an acceptable password, you will be asked to choose the Effective Date for the Key Record you are creating. While you have the option of choosing any date from today forward, you should choose today's date. The Key Record you are about to create will be in effect immediately, so by choosing today's date, you will know that any payments from this date forward were encrypted with this particular Key Record.



- ✓ Once you choose a date, Sumac saves the new Key Record into the Sumac database and shows it in your list on the screen.



Consequences of Creating The First Key Record

Now that there is a Key Record in the database, the credit card details in all payment records that are created and saved to the database will be encrypted using that Key Record. In addition, the payment information stored in Pledge records will immediately be encrypted using the new Key Record.

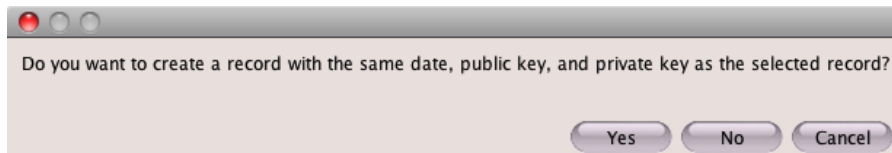
Create Copies of the Key Record For Other Users

After creating the first Key Record, all credit card payment data newly added to your Sumac database will be encrypted with the public key in that Key Record. Any user who needs to see payment data must have access to the private key in that Key Record, so that the user will be able to decrypt the payment information.

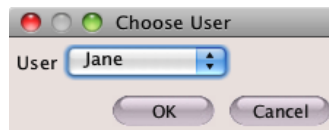
However, each Key Record is related to a particular user: it contains the user's log-on ID and a password. So you must define a Key Record for each user who needs access to payments. You do this by copying the original Key Record, creating a new one with the same public and private keys, but with a different user ID and password.

Here is how to make a Key Record for an additional user, with the same public and private keys as the one you just created.

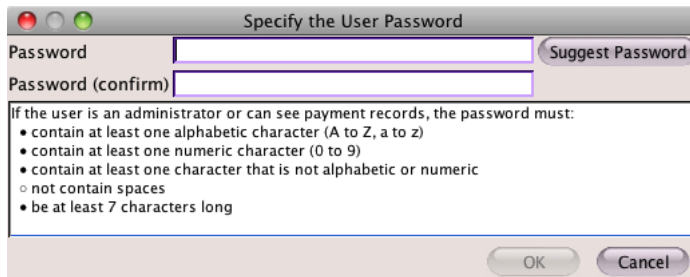
- ✓ In the Keys list window, click to select the Key Record that you wish to copy (one that was created earlier with your user ID). Click the New button. You are asked if you want to make a copy of the Key Record for a different user. Click Yes.



- ✓ Next, you must choose the user for whom you are creating a copy of the Key Record. Choose the user and click OK.



- ✓ You are then asked to enter a password. Specify the password that this particular user will need to enter for this particular Key Record. The password must satisfy all the criteria for viewing payment information, but does not need to be the same as the password used by the user to log on nor does it need to be the same as the password used to protect other Key Records.



The above steps create a Key Record for the additional user. Henceforth, when that user logs on to Sumac he or she will be asked to enter the password required to unlock his or her Key Records. Any payment information encrypted with the public key in this Key Record will be visible to the user

Create a New Key Record

When a Key Record has been used for a long time, the risk increases that a user's password may have been compromised. To maintain a high level of security, you must create a new Key Record no less often than once every 12 months.

To create a Key Record with new public and private keys, follow the same procedure that is described at *Create the First Key* on page 21, then create copies of this Key Record for other users, as described at *Create Copies of the Key Record For Other Users* on page 23. Note the following points about the Effective Date of a new Key Record:

- ◆ The Effective Date you choose must be later than the Effective Dates of all other Key Records in the database.
- ◆ While you have the option of choosing any date from today forward, you should choose today's date. The Key Record you are about to create will be in effect immediately, so by choosing today's date, you will know that any payments from this date forward were encrypted with this particular Key Record.

Consequences of Creating a New Key Record

The new Key Record has an Effective Date that is later than all other Key Records, so it will be used to encrypt all new payment information: all payment records that are created and saved to the database will be encrypted using the newly created Key Record.

In addition, payment information stored in Pledge records will immediately be encrypted using the new Key Record.

Delete Key Records

How to Delete a Key Record

You can delete a Key Record by clicking to select it, then clicking the Delete button:

- ✓ Log on to Sumac as an administrative user.
- ✓ Choose the Keys command from the Administrator menu.
- ✓ Click to select the Key Record that you want to delete. Unlike in other lists in Sumac, you are allowed to select only one Key Record at a time; multiple selection is not allowed.
- ✓ Click the Delete button.
- ✓ Click to confirm that you want to delete the selected record. Sumac confirms that it has deleted the record

Change of User Roles

When a user should no longer have access to payment information in the Sumac database, perhaps because he leaves your organization or changes job functions, then you must delete that user's Key Records. This ensures that the user will no longer be able to access payment information in the database.

Making Payment Information Inaccessible

Deletion of Key Records provides an extra level of protection to ensure that old payment information is not accessible. This topic is discussed in the chapter *Retention Period Policy* on page 29.

Any Key Records whose Effective Date is more than RP days prior to the Effective Date of the most recently created Key Record can be deleted. This is because your Retention Period Policy entails deleting old payment details that would have been encrypted with these old Key Records. Since all data encrypted

with these old Key Records has been cleared from the database, the old Key Records are no longer needed.

Delete old Key Records whose Effective Date is more than RP days prior to the Effective Date of the most recently created Key Record.

Deleting the Last One With a Particular Effective Date

If you delete the last Key Record with a particular Effective Date, then the credit card details in payments that were encrypted with that Key Record are no longer accessible because there is no longer a private key to decrypt them.

You should ensure that there is a Key Record with a later Effective Date before you delete the last Key Record with a particular Effective Date. This ensures that new payment information will be encrypted using a later rather than an earlier Key Record.

Payment Information in Pledge Records

Pledge records contain information about credit cards, so that the credit card can be charged each month. Because a pledge may cover several years, this information may stay in the pledge record for several years, much longer than a typical RP.

Whenever a new key pair is created in a new Key Record (see *Create a New Key Record* on page 23), Sumac automatically re-encrypts the credit card details in all pledge records using the new Key Record. This does two useful things:

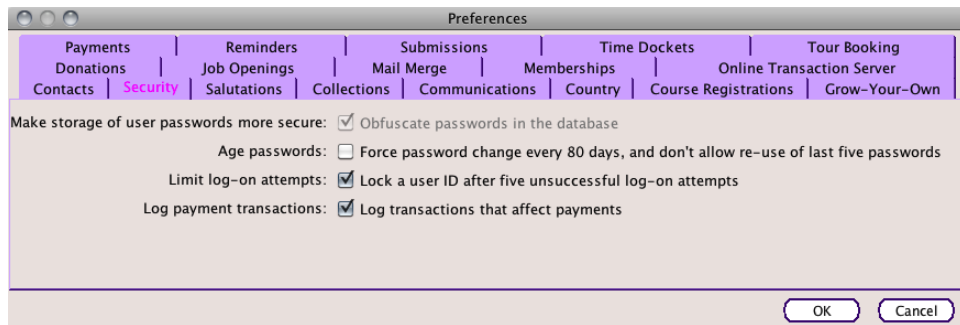
- ◆ It ensures that the pledge records are regularly re-protected with current security information.
- ◆ It makes sure that deletion of old Key Records will not affect pledge information.

Additional Security Features of Sumac

Preferences Command – Security Tab

Warning: In order to comply with PCI DSS you must turn on all the checkboxes in this dialog, enforcing password obfuscation, password aging, limiting log-on attempts, and logging payment transactions.

If you are a Sumac administrator, you can use the Preferences command in the Administrator menu. This command provides many tabs containing settings for configuring how different parts of Sumac function. Here is a picture of the Security tab, and an explanation of what each checkbox does:



<i>Check box</i>	<i>What it does</i>
Obfuscate passwords in the database	<p>Passwords stored in the user information table in the database are stored in clear (readable) text. If you obfuscate them, then they are converted to an unreadable format. For example if the user’s password is “password”, it will be converted to this:</p> <p>33898bfe627945675e103ea70a29a94383fe03ea05d13450f49a0602e6cedccaf</p> <p>The conversion uses a hash algorithm⁵ – a mathematical calculation that cannot be reversed. So even if someone sees the obfuscated password, he will not be able to determine what the password is.</p>
Force password change every 80 days, and don’t allow re-use of last five passwords	<p>This check box imposes two policies:</p> <ul style="list-style-type: none"> ◆ passwords must be changed at least every 80 days ◆ when changed, the new password cannot be one of the last five that have been used.
Lock a user ID after five unsuccessful log-on attempts	<p>If a user tries to log on five times, typing an incorrect password each time, then the user ID is locked until an administrator unlocks it.</p>

⁵ SHA-256

<i>Check box</i>	<i>What it does</i>
Log transactions that affect payments	This checkbox causes Sumac to record whenever a user adds, deletes, processes, or changes a payment record, or adds or deletes a key record. This log can be used to audit and trouble-shoot payment security issues.

Backing Up Your Database

It is imperative that you back up the data in your database. This data is very valuable, recording the past and providing the foundation for the future of your organization.

Single-user (Bronze, Silver) Databases

If you have a single-user (Sumac Bronze or Sumac Silver) database, then your data resides on your computer. You need to ensure that it is backed up on a regular basis, just like you should back up other files on your computer.

The most recent information about back-ups (why? how?) can be found in the Frequently Asked Questions at <http://sumac.com/support>.

Self-Hosted Multi-user (Gold) Databases

If you have a multi-user (Sumac Gold) database, then your data resides on a server computer. You need to ensure that it is backed up on a regular basis, perhaps at the same time as you back up other information on the server.

The most recent information about back-ups (why? how?) can be found in the Frequently Asked Questions at <http://sumac.com/support>.

Sumac Online

If you use the Sumac Online service, whether your database is Bronze, Silver, or Gold, then you do not need to worry about backing up your database.

The database is hosted at a professional hosting facility in Vancouver. It is automatically backed up in Vancouver once each day, and automatically backed up in Toronto twice each day. In addition, the Toronto backups are backed up to an off-site facility twice per week.

The backups are preserved for one month, and one backup per month is archived for backup prior to the current month.

Backup media are encrypted, so even if computers or media are stolen, your data is still protected.

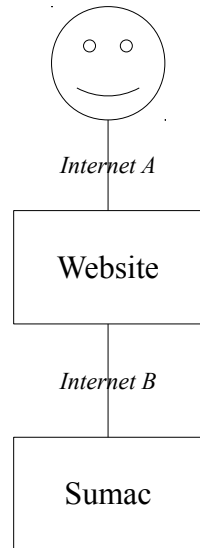
Your database is separate from that of every other organization and your database is backed up separately from all others.

Website Encryption

Warning: In order to comply with PCI DSS rules for protection of payment information, you must follow the procedures in this section.

Overview

If you have pages on your website which integrate with your Sumac database, sending data to it and retrieving data from it, then you need to protect credit card data as it passes through the Internet.



As a user (the top circle) enters payment information into your website, there are two points where the information is vulnerable, both moments when payment information is passed over the Internet.

The first, *Internet A*, is when the payer uses a browser to send information to your website. The second, *Internet B*, is when the website sends the payment information to Sumac for processing.

Protect the Internet A Connection

Any pages on your website that entail users entering passwords, personal identification information, or payment information should be in a secure area of your website. This means that these pages will be encrypted and use the https (instead of http) protocol. Usually the easiest and most cost effective way to secure an area of your website is to get encryption keys from the organization that hosts the website for you. This ensures that information from the user's browser is encrypted as it passes to your website.

Also, ensure that you are launching the pages with https, not just http. The https protocol uses encryption to protect data, but http sends data without using encryption.

Protect the Internet B Connection

If you use pages provided by Sumac, for integration between your website and your Sumac database, then the data is protected using a public-private key pair (see *Public and Private Keys* on page 19). The public key is in a .pem file that is part of your website. The corresponding private key is in a .jks file for your Sumac server.

The public key is used to encrypt the data sent from your website to Sumac. The private key enables Sumac to decrypt and use the data from the website.

When you first get the standard pages they contain a standard public-private key pair; this is convenient for testing since everyone can share the same keys. But before you go into production you *must* replace the key pair. If you have expertise in security, you can do this yourself, creating a .pem and .jks file with corresponding public and private keys. Alternatively, if you ask, your Sumac support organization will generate a key pair just for you and send the two files to you in a secure way.

Retention Period Policy

Warning: You must institute a retention period policy and its supporting procedures, as described in this chapter, in order to comply with the requirements of PCI DSS.

Introduction

One potential risk is that you may unnecessarily preserve credit card information in your database, long after it is no longer useful. This chapter outlines procedures to follow in order to avoid this risk.

Establish a Retention Period (RP)

Establish a retention period (RP). This is the number of days that payment information will be retained. A suggested number of days is the longest time after which a payment may be rescinded, plus 90 days. For example, if your agreement with your payment processor permits payments to be rescinded for up to 120 days, then RP would be 210 days.

Delete Old Backup Databases

You must ensure that you do not retain payment information in copies of your database for longer than RP. You must establish a regular procedure for deleting old backup files, to ensure that they are not retained longer than RP days.

Payment Information in the Sumac Database

On a monthly basis, remove payment details from Payment records in the database that are older than RP. Here is what to do:

- ✓ In the Payments list, search to find all payments dating from RP days ago to RP+60 days ago – payments whose payment information is still in the database but does not need to be.
- ✓ Click the Clear button and confirm that you want to clear payment details from all the payment records. This button clears credit card details from payment records, while still maintaining the other aspects (e.g. who made the payment, how much was paid, on what date) of the payment.

Key Management

Key Records are explained in detail in the chapter *Key Records* on page 19. That chapter describes procedures that must be followed on a regular basis to ensure the secure encryption of payment data stored in your Sumac database.

Payment Processing Security in Sumac

Introduction

This information in this chapter is provided to enable Sumac to conform to the PA-DSS standard. This standard specifies technology and documentation criteria to be met in order to ensure that payment information is protected. This standard is available from the PCI Security Standards Council at:

<https://www.pcisecuritystandards.org>

Summary

This documentation applies to Sumac releases 3.6 and later. Sumac is an application that runs on personal computers, storing its information in a database.

Supported Operating Systems

Sumac runs on all operating systems that support a Java Runtime Environment (JRE) 1.6 or later.

It is fully supported on Windows (2000, XP, Vista, 7), Mac OS X (10.5.2 and later), and Linux (selected variants).

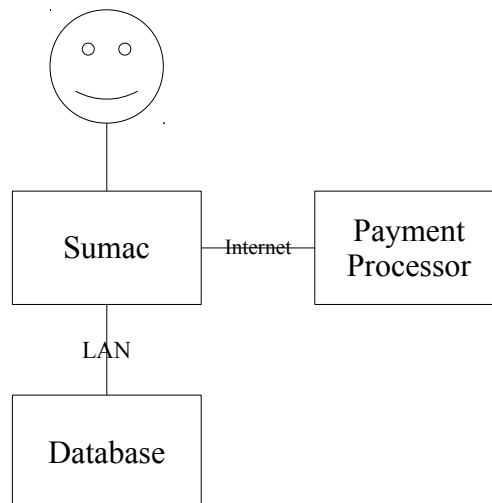
Target Industry and Customers

Sumac is intended for use by non-profit organizations.

Support Connections to External Processors and Card Brands

Sumac supports all card brands supported by the payment processors to which Sumac can connect. New payment processors are regularly added, but the list currently includes Beanstream, Blue Pay, Century Business Solutions, Elavon, and IATS. Connections to server computers, provided by these payment processors, are performed over the Internet.

Typical Implementation



In a typical installation, a user runs Sumac on his personal computer.

That personal computer connects to the database. The database typically resides on a computer in the same office as the user and is accessed over the local area network (LAN) in the office.

When the user asks for a payment to be processed, Sumac saves the relevant information in the database, and connects over the Internet to a payment processor.

Data Storage Locations

Sumac never puts cardholder data into files. It stores payment information in two places in its database:

- ◆ In payment records (database table `cfr_payment`), which record the details of a particular payment.
- ◆ In pledge records (database table `cfr_pledge`), which indicate how pledged payments will be made in the future.

	<i>payment records</i>	<i>pledge records</i>
What is stored:	<ul style="list-style-type: none"> ◆ cardholder name ◆ card type ◆ card number ◆ expiry year and month ◆ authorization code ◆ amount of payment 	<ul style="list-style-type: none"> ◆ cardholder name ◆ card type ◆ card number ◆ expiry year and month ◆ amount of payment
How it is protected:	All but the amount of payment is all stored in a single cell in the database, and is protected by encryption as described in <i>Key Records</i> on page 19.	All but the amount of payment is all stored in a single cell in the database, and is protected by encryption as described in <i>Key Records</i> on page 19.
How long this data is stored:	Until user procedures dictate that it should be cleared. See <i>Retention Period Policy</i> on page 23	Until the pledge period is over.
How the data is deleted when no longer needed:	The payment record can be completely deleted from the database. Alternatively, the payment record can be retained but the credit card information can be cleared from it.	It is deleted from the database when the pledge is completed and deleted.

CVV2 values, called *CC Verification Value* in Sumac, are the three-digit codes on the back of a most credit cards, or the four-digit code on the front of American Express cards. In Sumac, these codes can be entered into a payment record on the screen, and are used to process a payment, but they are never saved in the Sumac database.

Versioning Methodology

Sumac release version numbers are three numbers separated by periods. The second and third numbers are optional. Occasionally, an alphabetic character is added after the numbers.

Each release results in one of the numbers being incremented. When a number is incremented, the subsequent numbers are dropped for that release, to be added later. For example, if the current release is 3.5.2, and a major change requires the 3 to be incremented to 4, the release would be identified as release 4. The next release after that may be release 4.1, assuming the changes are appropriate for incrementing the second number.

If, for example, the release number is 3.5.2*b*, here is what causes each of the three numbers to be incremented:

First Number 3	This first number indicates a major change to fundamental aspects of Sumac. This type of change includes one or more of the following: <ul style="list-style-type: none"> ◆ extensive restructuring of the user interface ◆ major restructuring of the methodology used to distribute the application ◆ extensive restructuring of the database This type of change is visible to all Sumac users.
Second Number 5	Sumac functionality is divided into modules. This number is incremented when a major new module is added to Sumac, or when a module is extensively revised or enhanced. <p>This type of change is visible to all who use the affected module.</p>
Third Number 2	This number is incremented to indicate a release that incorporates minor enhancements. These may be extra capability added to a module, minor changes to existing capabilities, additional reports, improved dialogs or help sequences, etc. <p>This type of change is visible only to users who use the affected part of a module.</p>
Alphabetic <i>b</i>	Although we do our best to ensure that Sumac does not have bugs, sometimes we make a mistake. When this occurs, usually bugs are fixed in the next regularly numbered release. However, occasionally a bug has the potential to cause significant problems for Sumac users and necessitates an immediate release. Releases that do not warrant incrementing the first, second, or third numbers, are distinguished by a letter (<i>a</i> then <i>b</i> then <i>c</i> , etc.) being appended after the last number of the release.

Do not retain full magnetic stripe, card validation code, or PIN block data

Sumac does not support the entry or storage of these types of information:

- ◆ magnetic stripe data
- ◆ PINs
- ◆ PIN block data

Card validation values (CVV2, called *CC Verification Value* within Sumac) can be entered on the screen and are used when sending a transaction to a payment processor, but they are never stored.

For further details about how and where Sumac stores credit card data see *Data Storage Locations* on page 31.

PCI DSS Compliance

Introduction

What is PCI DSS?

PCI DSS⁶ is a standard for procedures to ensure that credit card payment information is kept secure. The standard is about 75 pages long and lays out numerous requirements as well as testing procedures to ensure that you satisfy the requirements.

You can download the PCI DSS from:
<https://www.pcisecuritystandards.org>

Why Bother?

Organizations that handle credit card payment data should comply with the PCI DSS. This ensures that the credit card data is protected and that your organization will not suffer the embarrassment of lost or stolen credit card data.

What's In This Chapter

This chapter lists *some* of the requirements of the PCI DSS. This chapter does *not* list all the detailed requirements, nor does it reproduce testing procedures or other materials that accompany each requirement in the standard.

Information quoted from PCI DSS looks like this:

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

Many of the requirements (e.g. those that relate to physical security of your offices) do not relate to your use of Sumac. However, where appropriate, beside each requirement there are comments about how Sumac helps you comply with the requirement.

Finally, while you should consider all the requirements of the standard, many apply only to configurations of computers that are more complex than those used by most non-profit organizations.

Build and Maintain a Secure Network

Requirements 1 and 2.

Requirement 1: Install and maintain a firewall to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

<i>Requirement</i>	<i>Application of Sumac</i>
1.1 Establish firewall and router configuration standards	
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	

⁶ Payment Card Industry Data Security Standard

<i>Requirement</i>	<i>Application of Sumac</i>
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	

Requirement 2: Do not use vendor-supplied defaults for system passwords

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

<i>Requirement</i>	<i>Application of Sumac</i>
2.1 Always change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	<p>Sumac provides both database and application level passwords. See <i>Access To Database – Passwords</i> on page 8.</p> <p>When defining user accounts you should keep these things in mind:</p> <ul style="list-style-type: none"> ◆ Give users only those capabilities they must have. Do <i>not</i> give everyone access to everything. ◆ Create a separate user ID for each user. Do <i>not</i> create shared accounts (e.g. a single account for all the volunteers).
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	<p>Sumac checks for new releases every time you run it. If there is a new release, you should install it to ensure that you have the most recent version of any security parts of the program.</p> <p>Sumac uses Java technology on all platforms (Linux, Macintosh, Windows). Make sure that you are using current Java technology, so that if any security vulnerabilities are found, you will get the fixes. To install the newest Java for your computer, go to:</p> <ul style="list-style-type: none"> ◆ http://www.java.com/getjava/

<i>Requirement</i>	<i>Application of Sumac</i>
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	<p>If you use a VPN connection to your office database, ensure that communication over the VPN channel is encrypted.</p> <p>Particularly relevant sections:</p> <ul style="list-style-type: none"> ◆ <i>Website Encryption</i> on page 27 ◆ <i>Database User IDs and Passwords</i> on page 9

Protect Cardholder Data

Requirements 3 and 4.

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

<i>Requirement</i>	<i>Application of Sumac</i>
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.	<p>To support your data disposal, Sumac's Payments list window provides a Clear button. This button clears credit card details from payment records, while still maintaining the other aspects of the payment.</p> <p>Particularly relevant sections:</p> <ul style="list-style-type: none"> ◆ <i>Retention Period Policy</i> on page 29 ◆ <i>Delete Key Records</i> on page 24
3.2 Do not store sensitive authentication data after authorization (even if encrypted).	Sumac does not store any sensitive authentication data (PINs, magnetic stripe data, card verification codes) after authorization.
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).	Sumac displays "*****" followed by the last four digits of the credit card number (PAN).
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:	<p>Credit card data is encrypted using 256-bit RSA encryption.</p> <p>Particularly relevant sections:</p> <ul style="list-style-type: none"> ◆ <i>Key Records</i> on page 19
3.5 Protect any keys used to secure cardholder data against disclosure and misuse:	<p>Particularly relevant sections:</p> <ul style="list-style-type: none"> ◆ all of the chapter regarding <i>Key Records</i> on page 19

<i>Requirement</i>	<i>Application of Sumac</i>
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	Particularly relevant sections: <ul style="list-style-type: none"> ◆ <i>Key Records</i> on page 19

Requirement 4: Encrypt transmission of cardholder data across open networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

<i>Requirement</i>	<i>Application of Sumac</i>
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.	<p>If remote users connect to your office network using a VPN connection, ensure that encryption is being used in the VPN connection. Make sure that you use good passwords on VPN connections.</p> <p>Credit card data being moved between Sumac program and the corresponding Sumac database is encrypted using 256-bit RSA encryption.</p> <p>Most Sumac installations entail access from a user computer, over a network, to a database that is on a server computer. The use of wireless networks makes it much more complex to validate security. Use wired connections to avoid security problems.</p> <p>If you connect your website to your Sumac database, then this section is particularly relevant:</p> <ul style="list-style-type: none"> ◆ <i>Website Encryption</i> on page 27
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	Sumac prevents you from generating messages with complete credit card numbers (PANs) in them. When you need to email this type of information (e.g. to confirm a purchase or donation made using a credit card), Sumac allows you to generate a message that shows “****” followed by the last four digits of the credit card.

Maintain a Vulnerability Management Program

Requirements 5 and 6.

Requirement 5: Use and regularly update anti-virus software or programs

Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

<i>Requirement</i>	<i>Application of Sumac</i>
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	
5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

<i>Requirement</i>	<i>Application of Sumac</i>
6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	Sumac checks for new releases every time you run it. If there is a new release, you must install it to ensure that you have the most recent version of any security parts of the program. Sumac uses Java technology on all platforms (Linux, Macintosh, Windows). Make sure that you are using current Java technology, so that if any security vulnerabilities are found, you will get the fixes. To get the newest Java go to: ◆ http://www.java.com/getjava/
6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.	
6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices.	
6.4 Follow change control processes and procedures for all changes to system components.	
6.5 Develop applications based on secure coding guidelines.	

<i>Requirement</i>	<i>Application of Sumac</i>
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks.	Particularly relevant section: <ul style="list-style-type: none"> ◆ <i>Website Encryption</i> on page 27

Implement Strong Access Control Measures

Requirements 7, 8, and 9.

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.

<i>Requirement</i>	<i>Application of Sumac</i>
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	If a user does not need to access payment data, then do not give the user access to this type of data. Note that a user can see donation and pledge data even if the user is not allowed to see payment details. Particularly relevant sections: <ul style="list-style-type: none"> ◆ <i>Access By Data Types</i> on page 14 ◆ <i>Create Copies of the Key Record For Other Users</i> on page 23 ◆ <i>Delete Key Records</i> on page 24
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	When you define a new Sumac user account, the user has no capabilities. You need to add capabilities as appropriate to each user's role. Give each user the fewest capabilities possible to accomplish his or her job. Particularly relevant sections: <ul style="list-style-type: none"> ◆ <i>Access By Data Types</i> on page 14

Requirement 8: Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

<i>Requirement</i>	<i>Application of Sumac</i>
<p>8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.</p>	<p>Every user of Sumac must enter a user ID before being able to access the database. In addition, each user must enter a password to unlock Key Records which are used to protect credit card information stored in payment records.</p> <p>Particularly relevant sections:</p> <ul style="list-style-type: none"> ◆ <i>Access To Database – Passwords</i> on page 8.
<p>8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:</p> <ul style="list-style-type: none"> ◆ Something you know, such as a password or passphrase ◆ Something you have, such as a token device or smart card ◆ Something you are, such as a biometric 	<p>Every user of Sumac must enter a password before being able to access the database.</p> <p>Particularly relevant sections:</p> <ul style="list-style-type: none"> ◆ <i>Access To Database – Passwords</i> on page 8.
<p>8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties.</p>	
<p>8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.</p>	<p>When password obfuscation is in use for Sumac user IDs and passwords, then passwords moved between Sumac and the database are always encrypted, and only the encrypted version of the password is stored in the database. Passwords that protect private keys in Key Records are always obfuscated.</p> <p>Particularly relevant sections:</p> <ul style="list-style-type: none"> ◆ <i>Password Obfuscation</i> on page 11 ◆ <i>Key Records in Sumac</i> on page 20 ◆ <i>Preferences Command – Security Tab</i> on page 26

<i>Requirement</i>	<i>Application of Sumac</i>
8.5 Ensure proper user identification and authentication management for non-consumer users and administrators.	<p>Only a user with Sumac administrative privileges is allowed to add users and change passwords. See <i>Access To Database – Passwords</i> on page 8.</p> <p>Once a user is no longer using Sumac, that user’s account should be deleted to ensure that the user can no longer access the database.</p> <p>Password changes by non-administrative users require confirmation of the current password before a new one can be set.</p> <p>There are no built-in user IDs or passwords that enable Sumac personnel to access your database.</p> <p>You can tell Sumac to force regular password changes. See <i>Password Aging</i> on page 12.</p> <p>If a user is allowed to see payment information, his or her password must be high quality. See <i>Password Quality</i> on page 12.</p> <p>Each Key Record is protected by a separate password which must be high quality. See <i>Key Records</i> on page 19.</p>

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

<i>Requirement</i>	<i>Application of Sumac</i>
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.	
9.3 Make sure all visitors are handled as follows: 9.3.1 Authorized before entering areas where cardholder data is processed or maintained. 9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel. 9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration.	

<i>Requirement</i>	<i>Application of Sumac</i>
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.	Particularly relevant sections: <ul style="list-style-type: none"> ◆ <i>Delete Old Backup Databases</i> on page 29
9.6 Physically secure all media.	
9.7 Maintain strict control over the internal or external distribution of any kind of media, including the following:	
9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	
9.9 Maintain strict control over the storage and accessibility of media.	
9.10 Destroy media when it is no longer needed for business or legal reasons	

Regularly Monitor and Test Networks

Requirements 10 and 11.

Requirement 10: Track all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

<i>Requirement</i>	<i>Application of Sumac</i>
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	
10.2 Implement automated audit trails for all system components.	You must tell Sumac to log all transactions that relate to payments. Once this feature is enabled, it is automatic. Payment transactions, and actions that affect the log, are logged automatically. Particularly relevant sections: <ul style="list-style-type: none"> ◆ <i>Preferences Command – Security Tab</i> on page 26

<i>Requirement</i>	<i>Application of Sumac</i>
10.3 Record audit trail entries for all system components for each event.	Sumac records this information in its payment transaction log: <ul style="list-style-type: none"> ◆ user ID ◆ date and time ◆ type of operation ◆ payment record affected
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	Servers can typically have their clocks set using a recognized standard. Entries in Sumac's payment transaction log are time stamped using the time on the server, not on the Sumac user computer.
10.5 Secure audit trails so they cannot be altered.	Only Sumac users with administrative privileges and the ability to see payments (based on their user access privileges) are able to see the payment transaction log. The log entries cannot be changed and entries cannot be deleted. Backup of the Sumac database should be automated so that the log, along with other data, will be saved at regular intervals.
10.6 Review logs for all system components at least daily.	An administrative user can use the Payment Transaction Log in the Administrative menu to review logged information.
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).	Entries in Sumac's payment transaction log are kept indefinitely.

Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

<i>Requirement</i>	<i>Application of Sumac</i>
11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.	Most Sumac installations entail access from a user computer, over a network, to a database that is on a server computer. The use of wireless networks makes it much more complex to validate security. Use wired connections to avoid security problems.

<i>Requirement</i>	<i>Application of Sumac</i>
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	
11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.	
11.5 Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	

Maintain an Information Security Policy

Requirement 12.

Requirement 12: Maintain a policy addressing information security for all personnel

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

<i>Requirement</i>	<i>Application of Sumac</i>
12.1 Establish, publish, maintain, and disseminate a security policy.	Particularly relevant sections: <ul style="list-style-type: none"> ◆ <i>Retention Period Policy</i> on page 29 ◆ <i>Key Records</i> on page 31
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	

<i>Requirement</i>	<i>Application of Sumac</i>
12.3 Develop usage policies for critical technologies (for example, remote- access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies.	
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	Particularly relevant sections: <ul style="list-style-type: none"> ◆ <i>Retention Period Policy</i> on page 29
12.5 Assign to an individual or team the following information security management responsibilities:	
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)	
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	Cardholder data stored in Sumac cannot be exported so it cannot be shared with other service providers.
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	

– End of Manual –