mSIS Security Policy and Protocol

Introduction

This Policy details the secure use of mSIS as a tool for the capture and reporting of internet intelligence and investigations (i3).

- mSIS is a powerful i3 software application developed and owned by Qwarie Ltd.
- mSIS allows the researcher to capture, protect and secure personal data and evidence during an investigation, and to distribute that personal data and evidence securely, through the mSIS reporting function, so that the whole process might be compliant with current legislation.
- mSIS allows the user to apply best practice security controls against unauthorized access and the modification of personal data and evidence throughout the judicial process of capture, disclosure and prosecution.

This Policy should be read in conjunction with the mSIS Data Protection Compliance Statement.

Scope

Part 1: Data Security

Part 2: Process Security

Part 3: Evidence Security

Part 1: Data Security

Qwarie applies the following secure practices for the capture of personal data:-

1.1. Login Credentials

The Customer organisation shall assign at least one Administrator with responsibility for login credentials of each licence user.

The Customer Administrator shall be obliged to provide a login for each licensed user, with the following protocol.

Usernames with the following format: xxxx-yyyy-zzzz, where;

- xxxx is an acronym of the Customer organisation with no more than 4 characters, and where;
- yyyy is the initials of a name of the researcher, or of the false persona used for research, with no more than 4 characters, and where;
- zzzz is a 4 digit numeric code, that shall render the user-name unique, and, so that;
- the 3 sections of the user-name shall be separated by a hyphen "-" character.

Passwords shall have a minimum of 12 characters. Qwarie recommends a strong password (that contains lowercase and uppercase letters, numbers, special characters). A story based passphrase, created by the user, should be easy to commit to memory.

The Customer Administrator shall provide to Qwarie, one username for each single user licence procured, and;

For each multi-user licence, the Customer Administrator shall provide to Qwarie, a quantity of usernames, as agreed between the Parties.

The Customer Administrator shall maintain a record of each licence username.

The Customer Administrator shall have the right to modify a login.

Customer Researchers, who are the licensed users, shall not have the right to modify a login.

The Customer Administrator is obliged to make a secure record of each login and shall be responsible for password recovery.

Login credentials should be applied into the Qwarie CRM or, transmitted through secure communication (see sub-section 1.2. of this Policy).

1.2. Secure Communication

Qwarie provides secure communication of User login credentials, with the Qwarie CRM.

Alternatively, Qwarie provides a public key for secure e-mail communication.

The Qwarie public key is published on https://www.qwarie.com/documents

Where a Customer has a public key, it should be made available to Qwarie, so that the Parties might communicate with secure e-mail.

Where the Customer does not supply an option for a secure e-mail, so that Qwarie is obliged to communicate with unsecure e-mail, there are alternative channels for secure communication that are:-

- Signal client, and;
- WhatsApp client, and;
- SMS.

Also, the Customer may elect to save a file within a Zip Archive and apply a password to the Archive, transmit the Archive to Qwarie by e-mail and send the password by SMS or other secure means (see above).

1.3. Secure authentication

Each Customer Researcher user is identified through the authentication process, so that the user is validated as a legitimate and authorised user with rights to conduct research and create an evidence report.

Authentication functions are implemented through the following process:-

- to authenticate the login to mSIS, the credentials are sent to a Qwarie server;
- where the username & password combination is correct, and the account has an active subscription, access to mSIS is granted;
- each day, mSIS checks with the Qwarie server to verify that a subscription attached to an account is still active;
- as with the login process, the username and password are sent to the Qwarie server for verification;
- login credentials are stored by Qwarie;
- login data may be requested from Qwarie.

2. Encryption

Encryption is the method by which any type of data is converted from a readable form to an encoded version that can only be decoded by another entity, where they have access to a decryption key.

Encryption is one of the most important methods for providing security, and does not allow attackers to compromise passwords and login credentials.

- The only data that is sent by mSIS to any Qwarie server are login credentials;
- mSIS stores the credentials in a database on a secure server;

- Data is communicated to any Qwarie server over an encrypted connection, using the TLS 1.2 cryptographic protocol;
- Backup of the database, that stores the login credentials, is performed daily.

3. Public Key

Public keys are used to convert a message into an unreadable format. Decryption is carried out using a different, but matching, private key. Public and private keys are paired to enable secure communication.

Part 2: Process Security

For the management of mSIS licences, the Customer shall create an account in the Qwarie CRM, and authenticate with the following types of user:

(a) Customer Administrator

(b) Customer Supervisor (optional)

(c) Customer Researcher

To create a Customer Administrator account, the Customer shall provide the Customer entity name, the name of the Customer Administrator and an accessible e-mail address. This is the only personal data that Qwarie shall store.

Qwarie has no requirement to store any personal data of an mSIS user, therefore Qwarie requires obfuscated usernames for the security and privacy of a licensed user (see sub-section 1.1 of this Policy).

Where mSIS is deployed to perform research, each individual search that a licensed user performs is recorded in the Audit Log, including the username, therefore;

The obfuscated username shall conceal the identity of the user, so that the personal information of the user remains protected and does not display in the Audit Log.

The Customer Administrator shall maintain a record that maps each username to the real name of each licensed user.

Part 3: Evidence Security

Qwarie has no access to the evidence gathered during the research process, so that:-

3.1. Evidence storage on a local drive of the user

Where mSIS is deployed, all research performed by a logged-in user and every element within a Case Bundle, is saved locally, onto the user's computer, or networked drive.

- No data is saved to a Qwarie server, or any other external server, and;
- No data can leak to Qwarie, or any other external server.

Furthermore, where mSIS is deployed to perform research, the local browser might be set-up at the user's discretion, to keep a history of pages visited and cookies delivered. These records are saved on the user's local computer or networked drive.

No data capture is sent to Qwarie, or is accessible by Qwarie, or any other party.

Each Case Bundle might include an evidence sheet and a report in PDF & HTML format, with an Audit Log, a decision log, a Hashes folder, and an Attachments folder with all screenshots and attachments gathered during the research process.

These records are saved to the user's local computer or networked drive. No data is sent to Qwarie, or is accessible by Qwarie or any other party.

3.2. Audit Logs

Where mSIS is deployed, the Audit Log contains a record of each individual search that is performed by a user.

Where the browser history is deleted, the only record of the pages searched, is recorded in the Audit Log.

The Audit Log is saved and stored within the Case Bundle, as an HTML file type.

The user may export the Case Bundle outside of mSIS, onto the user's own computer, or networked drive, and to any other server as determined by the user.

3.3. Hashes File

Hashes ensure that data gathered shall not been tampered. The following measures have been implemented into mSIS:-

- where exporting a Case Bundle, a new file, “hashes”, is created with an HTML format, that contains all report resource hashes;
- at the point of the case export function, a file title shall generate stating, “A hash file has been generated by ”username “+ “at” + timestamp “;
- also, the hashes file shall generate with an image version, so that any edit of a hashes file might be difficult to edit.
- both HTML and image, hashes files are saved to a hashes folder, that contains individual files from all the Case exports that have been made during an investigation;
- when importing a Case Bundle, it is verified that the hashes of all files inside the Case Bundle match the values inside the hash file, and;
- where the values inside a hashes file might differ, a pop-up warning message shall display that shall allow the user to, either deny or continue with the import of a case bundle into mSIS.

3.4. Case Bundle Naming

- Each Case Bundle export shall be named and with an appended time stamp and the initials of the user;
- The user might choose between case name or case number for the Case Bundle name;
- Where a naming setting is applied, it shall hold true for all new Case Bundle naming until the setting is modified;
- The name applied to the Case Bundle shall be appended to any Evidence sheet, Report.pdf, Attachments folder, Archived folder, Audit Log and Hashes folder;
- Within each folder, files shall be appended with the case number, except for;
- the Case Bundle json configuration file, that be named DoNotModify.json.

Notification of changes to this Policy

From time to time, Qwarie may make changes to this Security Policy and Protocol, to reflect any changes in security practices in compliance with legislation, best practice and technology enhancements. To be notified of changes to this Policy, please subscribe to the Qwarie e-mail list.
