Public Safety Business Agency:

Public Submission: Operation Impala

Submission No. 1

SUBMISSION OF Timothy DILLON

Name of Witness Timothy Joseph Dillon	**Date** 13 November 2019
Address of Witness C/- Public Safety Business Agency, 30 Makerston Street, BRISBANE QLD 4000	**Age (DOB)** [redacted]
Occupation of Witness A/Director Digital Transformation, Frontline Digital Services, Public Safety Business Agency, 30 Makerston Street, BRISBANE QLD 4000	**Telephone Nos.** **Home:** **Business:**
	Telephone Nos. **Business:** [redacted]

Preamble

My full name is Timothy Joseph Dillon. I live at an address known to the CCC. I am employed as the Acting Director of Digital Transformation, Public Safety Business Agency, (PBSA), located at 200 Roma Street, Brisbane, QLD 4000. I have been employed with PSBA since its inception in 2014. Prior to PSBA I was employed with the Queensland Police Service (QPS) for three years, also in the technology area. Prior to that I was contracted by Queensland Police to work on Corporate Audit Project for 6 years. I have spent most of my early working life in analysis, programming and technology delivery and still use those skills in the managerial role I now hold.

I have a Bachelor of Information Technology in System Development and a Bachelor of Human Resource Management and other qualifications. The majority of my working career has been in the information and technology field.

I joined the Corporate Audit Project area at the QPS around 2006 when the Queensland Police Records and Information Management Exchange (QPRIME), was being introduced to the QPS as their main information database. There were several other interface and integration systems introduced about the same time. I have a thorough working knowledge of QPRIME audit and related expectations for investigations. PSBA is a service supplier to QPS with regard to IT systems and in my case, I manage the Corporate Audit Facility team.

A considerable number of QPS systems have audit trails and logs, but this submission is limited to QPRIME and QLite.

At this stage the audit systems are a record of activity and investigations are reactive to authorised requests by investigators with approved access to the investigation tools. We have requested that Niche make some changes to the audit trail to improve its data management to allow access by a wider range to tools to allow proactive investigations and predictive analytics.

Part 1 –QPRIME Logon - Splash Screen

When a qualified user logs into QPRIME the first screen they are presented with the following screen, see Figure 1;

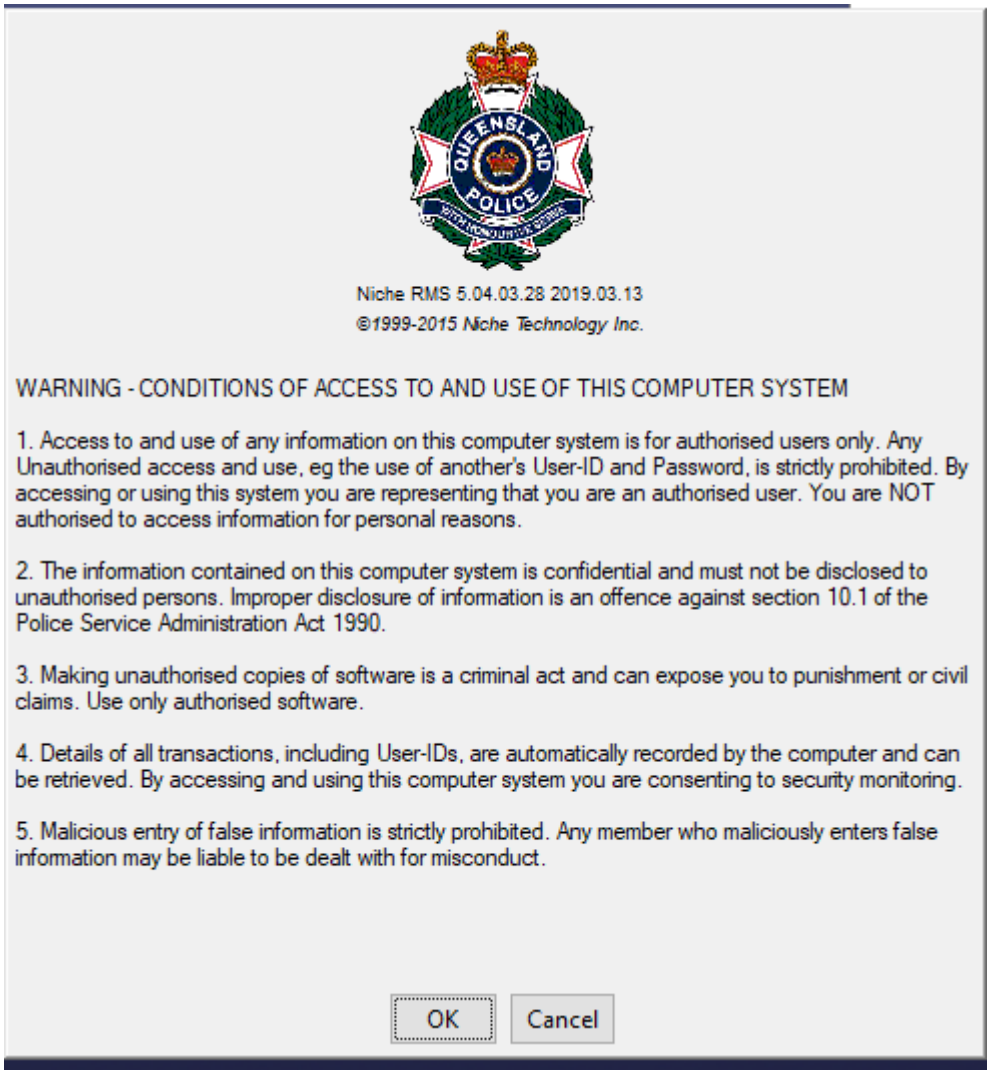


Figure 1 – Start up screen

This screen dictates the conditions of access and related instructions and warnings. The audit action on this screen is to record that OK has been pressed. If Cancel is pressed the user returns to the desktop. This screen is seen once at logon.

Part 2 – Reason for Access – QPRIME System

After the start up screen the user is presented with a mandatory Reason for Access screen. There are several aspects to note on this screen. See Figure 2;

1. The user/inquirer is prefilled as this is the logged-on user;
2. Next the user must select a Reason. This is a mandatory field and the choices are illustrated in the next screen, Figure 3;
3. Additional remarks can then be entered to further explain actions and intent as required. This is also a mandatory field but free form, so content is up to the user and may vary.
4. This reason can be changed (in a session) when a user is logged on to reflect alternate tasks. It can be invoked again on demand but is a user action. I understand that some work is underway to introduce this screen on other occasions.

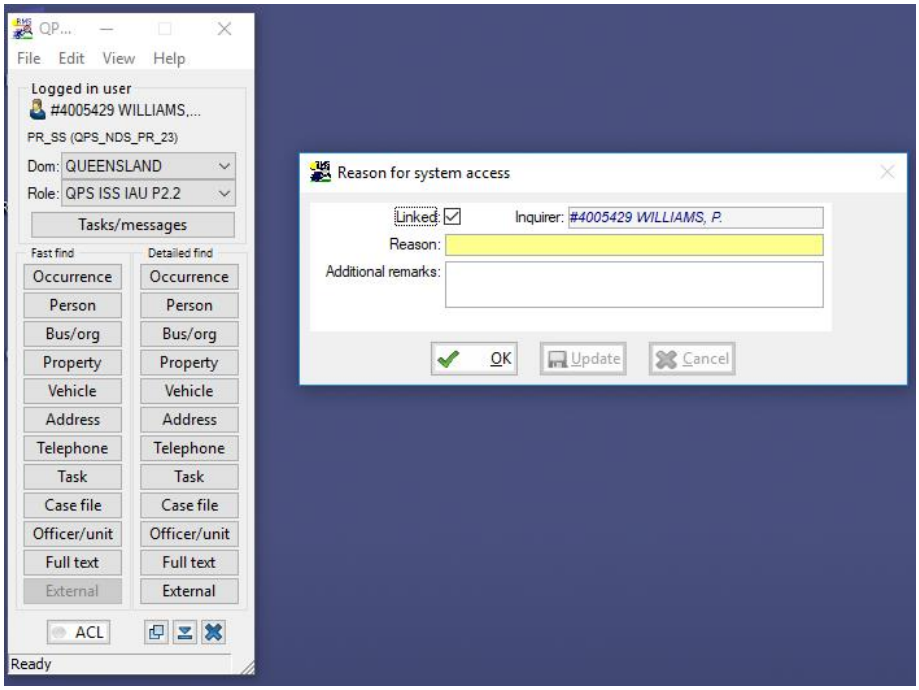


Figure 2 – Reasons for Access

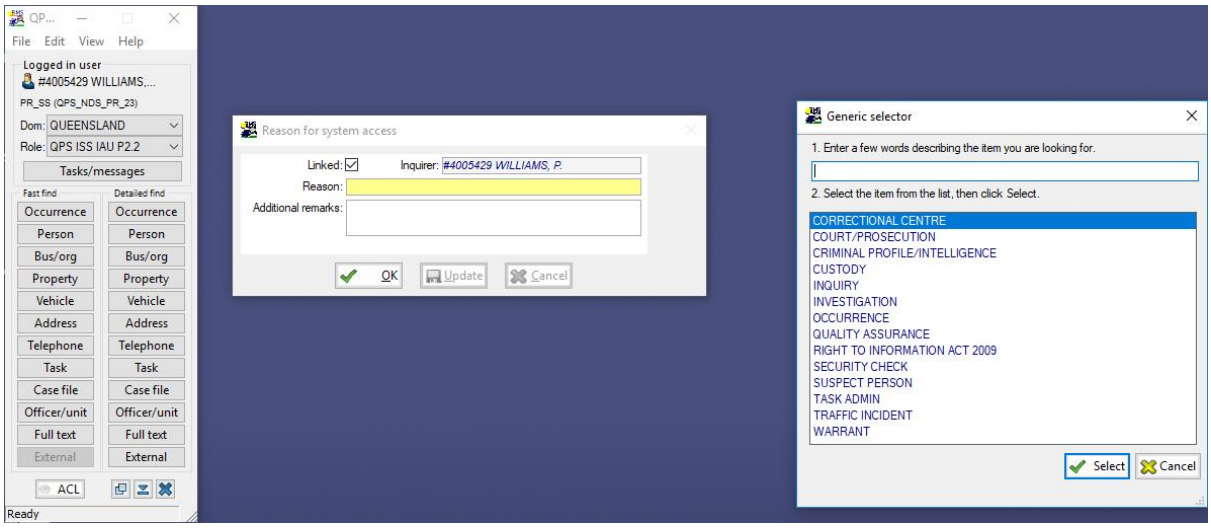


Figure 3 – Reasons for Access selection list

The audit action on this screen include and retain the details of; the user, Reason and Remarks when OK is pressed. If Cancel is pressed the user returns to the desktop.

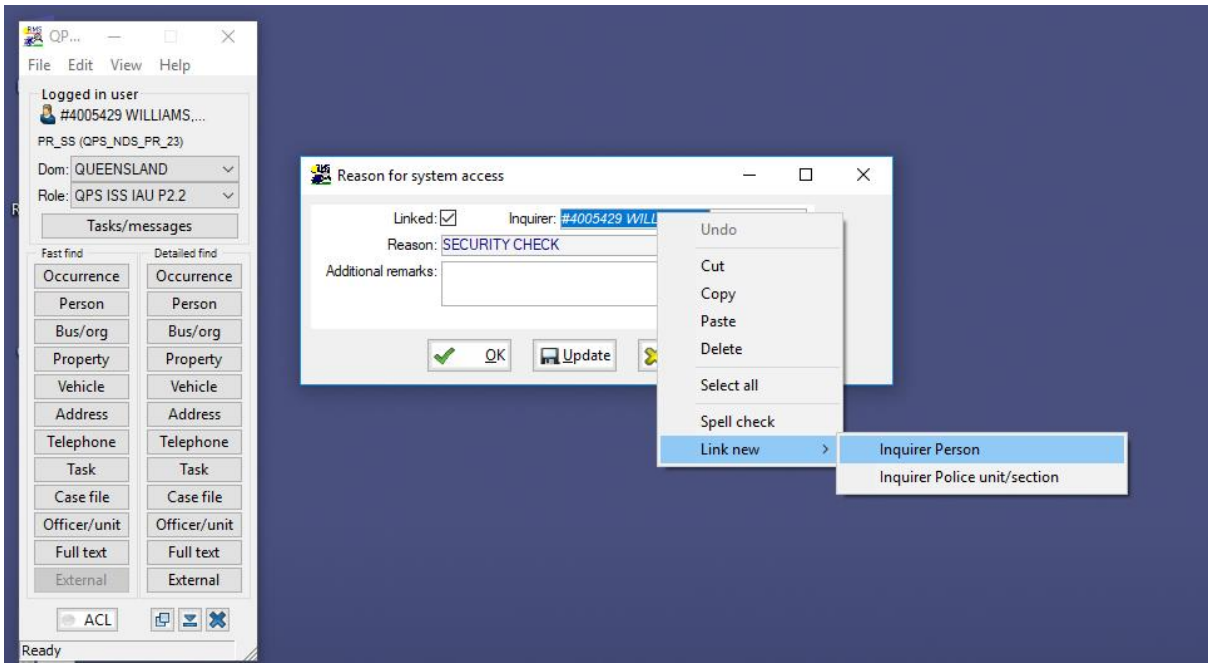
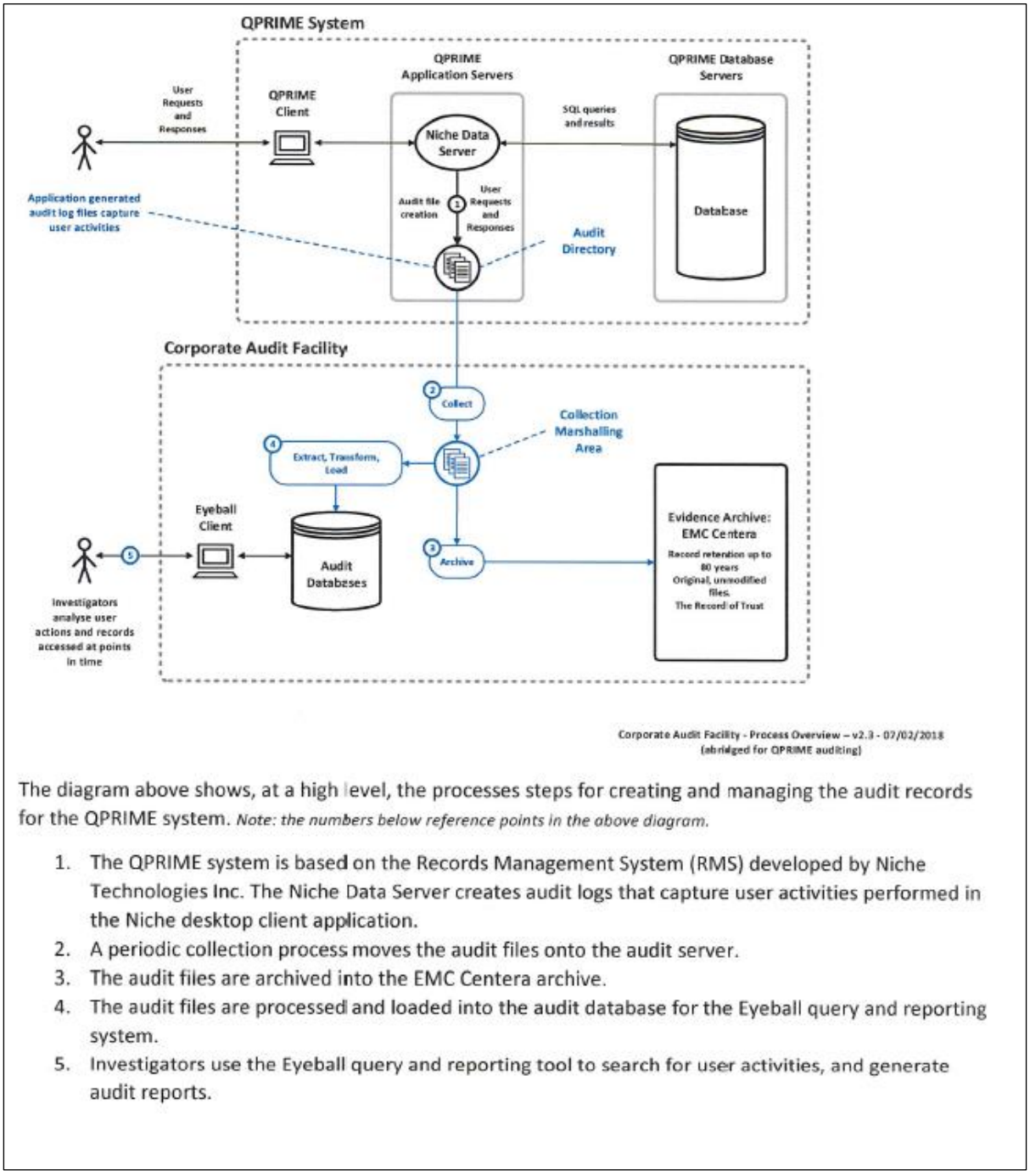


Figure 4 – On Behalf Of / Link an Inquirer

5. A further use case of Reason is on behalf of another. E.g. when responding to a phone or radio request from another officer or authorised person. As seen in Figure 4.

The audit action on this screen is to record the Reason and Remarks when OK is pressed. Both the original user and the selected inquirer are both recorded. These details and fields are stored and searchable. These are standard fields in investigation enquiry and report capability.

Part 3 – High Level QPRIME Audit Diagram



The diagram above shows, at a high level, the processes steps for creating and managing the audit records for the QPRIME system. *Note: the numbers below reference points in the above diagram.*

1. The QPRIME system is based on the Records Management System (RMS) developed by Niche Technologies Inc. The Niche Data Server creates audit logs that capture user activities performed in the Niche desktop client application.
2. A periodic collection process moves the audit files onto the audit server.
3. The audit files are archived into the EMC Centera archive.
4. The audit files are processed and loaded into the audit database for the Eyeball query and reporting system.
5. Investigators use the Eyeball query and reporting tool to search for user activities, and generate audit reports.

Figure 5 – QPRIME Audit Diagram

This diagram was prepared as part of witness statement for the CCC in Feb 2018 and describes the current process for QPRIME Audit.

Part 4 – QPRIME Audit Process

The following is an extract from the *statement of witness* that was prepared by me for CCC in Feb 2018. It still holds true today to describe the QPRIME Audit activities. Details about me have been are in the preamble.

_____ *extract starts* _____

4. The QPRIME system was a Records Management System developed and sold by a Canadian company called Niche Technologies Inc., which is for law enforcement agencies and is used by numerous law enforcement agencies world-wide.I have a very thorough working knowledge of how the Niche and QPRIME systems operate as I was part of the project team that developed an audit system for the QPRIME system to deliver an audit capability for the QPS. The Niche system is a bespoke police management system that came with an auditing feature but the Niche tool that interrogated that system was not able to meet the QPS requirements. QPRIME contains the Niche system but is also surrounded by other police interfaces and systems that make up the whole of QPRIME.
5. That integration and interfacing policing system connects to and integrates with other QPS systems, Queensland Government systems and Federal Policing systems. For example, there are fingerprint, media, and forensics systems also feeding off the Niche system in QPRIME. QHEALTH, Corrections, Main Roads and the Justice Department who are some of the State Government agencies that also integrated into Niche.
6. The Project managed the Niche audit trail collection and moved logs to a preserved secure area. Then those records are analysed, decomposed and coded to allow searching and activity-based audits. That data becomes information that is loaded into a system we developed named the Eyeball. I was also involved in the development of the Eyeball system and led a lot of the analysis, development and system testing for the loading process and its searching and display in Eyeball.
7. A QPRIME user logs onto QPRIME and then undertakes an activity, which could be numerous things and includes searching databases, displaying records, updating records, printing records. These activities and the response are recorded in the audit trail within Niche and is called an NDS audit log. That is a Niche feature. One of the Niche rules is that, if it cannot write the activity audit log successfully then it will not run or display anything to the client, other than an error message which is a fail-safe built in by Niche.
8. Those audit logs are held on a Niche server and are created periodically as you cannot collect the audit whilst the log is open. Old logs are collected after the new logs are created periodically either hourly or half hourly as dictated by the system configuration.
9. The next process is that those logs are collected and moved from Niche Servers into the Corporate Audit facility. Those records are considered the 'records of trust' and it is important that they must be preserved. They are then archived to an evidence archive where they have a retention period of up to 80 years. The system for that retention is called the EMC Centera, which is a technology system widely used in the corporate world which the QPS has chosen for this purpose. The logs in the EMC Centera system are locked away, like a vault in essence. That is then the record of trust now preserved. A copy of any log can be recalled from the Centera using a defined, secure process.
10. The stored logs are also processed by an Extract Transform and Load (ETL) process which stores the Niche logs into an audit format. This audit facility is the sum of all logs that have been collected and processed for the system time. The Niche database will then only show the

current record, but the Audit Database will show the history of any changes made from the creation, read and update of the activities. These activities in QPrime are all recorded by time and user and that is what the investigators use. Everything in the audit database is traceable back to two places. Back to the QPRIME system and the audit record of trust. The information in this database will show what the original activity was and any subsequent changes including who made those changes and when those changes were made.

11. The audit database is much larger than the original QPRIME database as it has all of the history of all the activities.
12. All the QPRIME activities which have become the records of trust are then retained in the EMC Centera for 80 years allowing for the statute of limitations of 72 years in Queensland and cannot be altered during that time.
13. As required, information such as logs can be extracted from the Centera which retain the activities and can be provided to qualified analysts to analyse. The Eyeball system is a Police bespoke system, no one else has it currently that I am aware of. That is where authorised QPS investigators conduct searches based on time, user activity or Niche Identifier (NID) which is a unique identifier for every Niche record preserved. The query on Eyeball could be related to a variety of search parameters. The results of those searches gives a report of the activities queried by the investigator. Everything that comes back from that NID query is preserved as at the point in time the original activity took place in Niche. I was part of the Eyeball Development project and was pivotal in the testing regime of the system.
14. I can categorically say that when someone undertakes an activity within QPRIME, and the system is operating normally and records that activity, that activity is auditable, transparent and preserved. The records returned from that original activity by the QPRIME user, will be identifiable from the audit trail that is ultimately available from the Eyeball queries conducted and can be validated against the source audit trails if required. The core information from Eyeball queries conducted will be exactly the same as that originally entered into Niche but may be in a different format to make it readable for consumers, ie police officers and other investigators.

_____ *extract ends* _____

Note that the retention period is stated in the above extract for 80 years, as this was the retention rule in place when the Centera archive was established. This has been reduced to 20 years and newer records are following this policy. I understand that this exceeds the record keeping standard.

Part 5 –QLite Logon - Splash Screen

QLite is a QPS mobility tool that enables officers to complete several police activities including searching QPRIME database and attached systems via integration. QLite runs as an application on mobile devices and has strong security access controls.

The user must complete the following screen to access QLite. These details are recorded in the QLite audit trail.

Figure 6 – QLite Credential Screen

Part 6 –QLite – Terms and Conditions

After the successful login the Terms and Conditions of use are then displayed. This screen cannot be bypassed, and its acknowledgment is recorded in the QLite audit trail.

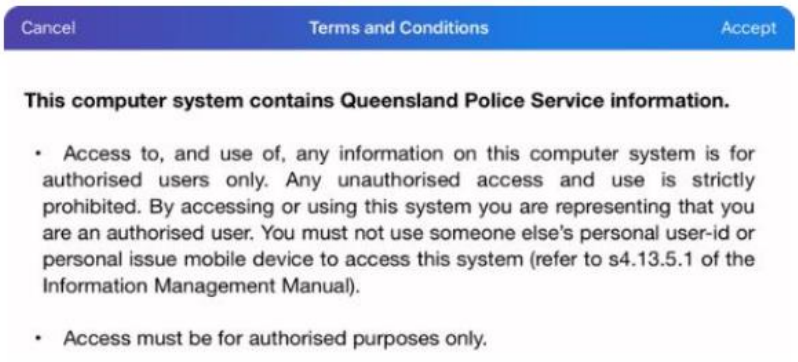


Figure 7 – QLite Terms and Conditions

Part 7 –QLite – Audit

QLite audit happens in two ways, the QLite actions on the device are recorded in its own audit trail that is collected, preserved and processed for investigation. The second layer of audit is that QLite uses the QPRIME interfaces and integrations to access information. These actions are recorded in the QPRIME audit trail described above.

IS18 and related notes

PSBA has strong policy relating to information security. These and all supporting policies are written to be consistent with the information security standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013 and are compliant with the Queensland Government's Information Standard 18: Information Security (IS18) and the Queensland Government Information Security Policy – Mandatory Clauses requirements.

PSBA Cyber Security unit is delegated to manage these policies, their implementation review and application. These principles were kept in mind when designing Audit systems, all QPS audit data is Protected and appropriate controls are in place.