4. How does QPS monitor special or high privileges in terms of access to their information asset in the above datasets?

QPRIME - Please see above, this is achieved through individual NAC Roles and ACLs applied to records.

QCAD - All users have the ability to see all data.

The only exception is when a QCAD Incident is "hidden" from view due to a restriction applied as authorised by an Inspector Communications Group, Community Contact Command upon request. This function to restrict an incident rests with CAD Support, Core Systems, Organisational Capability Command.

NCOS – Registrar Access can be considered as special or high privilege access of NCOS. Registrar Access is granted to the State Registrar, Registry Officers and Intel officers who perform functions in the administration/management scope as per the Child Protection (Offender Reporting and Offender Prohibition Order) Act. Investigators/Police officers outside of the Registry who have NCOS access do not have this level of access. The State Registrar authorises who can have high privilege access depending on the role they perform.

DCSYW 'Our Child' – not applicable. There are no special or high privileges in terms of access

IMAC - All user access regardless of privilege is logged by the system. The system provides a number of inbuilt system audit tools to examine and interrogate these logs.

5. Does the department monitor access to sensitive information (including information pertaining to vulnerable persons and high-profile persons)? If so, please explain how with specific examples (including if flags when information is accessed and random or regular audits of sensitive information). What does your department's category of vulnerable persons comprise of? (eg. domestic violence victims).

QPRIME - QPRIME does not specifically restrict or categorise records relating to vulnerable or high profile persons. This reflects the nature of policing and prevalence of dealing with people who may fall within the vulnerable categorisation. The option exists for notification of attempts to access entities to which an ACL has been applied. This option is exercised on a case by case basis and in certain circumstances such as records relating to covert identities and operations.

- The term 'vulnerable person' to indicate a person who is in need of assistance or protection due to their personal circumstances, and who may require a more nuanced or considered policing approach. Being vulnerable is not limited to one particular group of society – people from all walks of society can experience vulnerability at some time in their life – it can be temporary or permanent.
- This is reflected in the Service's Police Referrals network – the use of Police Referrals by Queensland Police officers has become an embedded strategy in the police response to all occurrences and is reflective of the Strategies and Opportunities identified in the Queensland Police Service Strategic Plan 2019-2023. Police are now able to refer directly to over 480 service providers covering 70 different issues which are broadly grouped into 22 referral categories. In 2018 police officers submitted 85,187 referrals for at-risk individuals to support services such as domestic and family violence (support for aggrieved and respondents), court support, parenting, victims assist, aged support, homelessness and mental health.

- In relation to vulnerable persons categories, our Unit covers the portfolio areas of: domestic and family violence; elder abuse; mental health / suicide prevention; disability; homelessness.
- Police Referrals and Victim Assist Queensland also fall within the DFV&VP Unit.

IMAC - The system maintains a log for every record created, accessed or modified regardless of the security applied and the system provides a number of inbuilt system audit tools to examine and interrogate these logs.

6. How does the QPS monitor authentication failure in the above datasets? E.g. user access denials and confirmation failures.

QPRIME - Please refer to previous response. The option is available to create notification for attempts to access records/entities to which an ACL has been applied.

QCAD - NA – user access is authenticated by their QPS Windows log-in. There is no extra password required for QCAD access.

NCOS – No functionality

DCSYW – 'Our Child' All employees with a valid QPS email have access to the portal. Identity management is maintained using Azure B2C identity federation services. Liaison on this is between DCSYW and PSBA IT services.

IMAC - Access to IMAC is controlled by the services Active Directory framework, therefore users may logon using their standard QPS computer account credentials.

The system logs all login attempts regardless of their resulting status. The system provides a number of inbuilt system audit tools to examine and interrogate these logs.

7. How do access controls to the above datasets adequately protect vulnerable people e.g. DV victims?

No additional protections are applied for vulnerable persons beyond the general framework provided through Information Security Policy and conditions of access to the system. This is reinforced through the capacity to record and audit individual user activity.

8. How does QPS perform user account and access reviews for the above datasets? How often does QPS undertake this review? Does the review include the following? Please explain:

- review of all user access rights on periodic basis
- review of privileged access rights on periodic basis
- regular monitoring to identify and remove any redundant / inactive account? E.g. account not used in the past 90 days?